INL/MIS-22-68905-Revision-0

Security and Resilience Implications of 5G for Aviation Subsector

September 2022

Arupjyoti Bhuyan, Sneha Kasera, Mingyue Ji

Changing the World's Energy Future

INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC

INL/MIS-22-68905-Revision-0

Security and Resilience Implications of 5G for Aviation Subsector

Arupjyoti Bhuyan, Sneha Kasera, Mingyue Ji

September 2022

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

Arupjyoti (Arup) Bhuyan

Technical Director, INL Wireless Security Institute (WSI)

Sneha Kasera

Professor, School of Computing, University of Utah

Mingyue Ji

Associate Professor, Electrical and Computer Engineering Department, University of Utah

Security and Resilience Implications of 5G for Aviation Subsector

INL Idaho National Laboratory

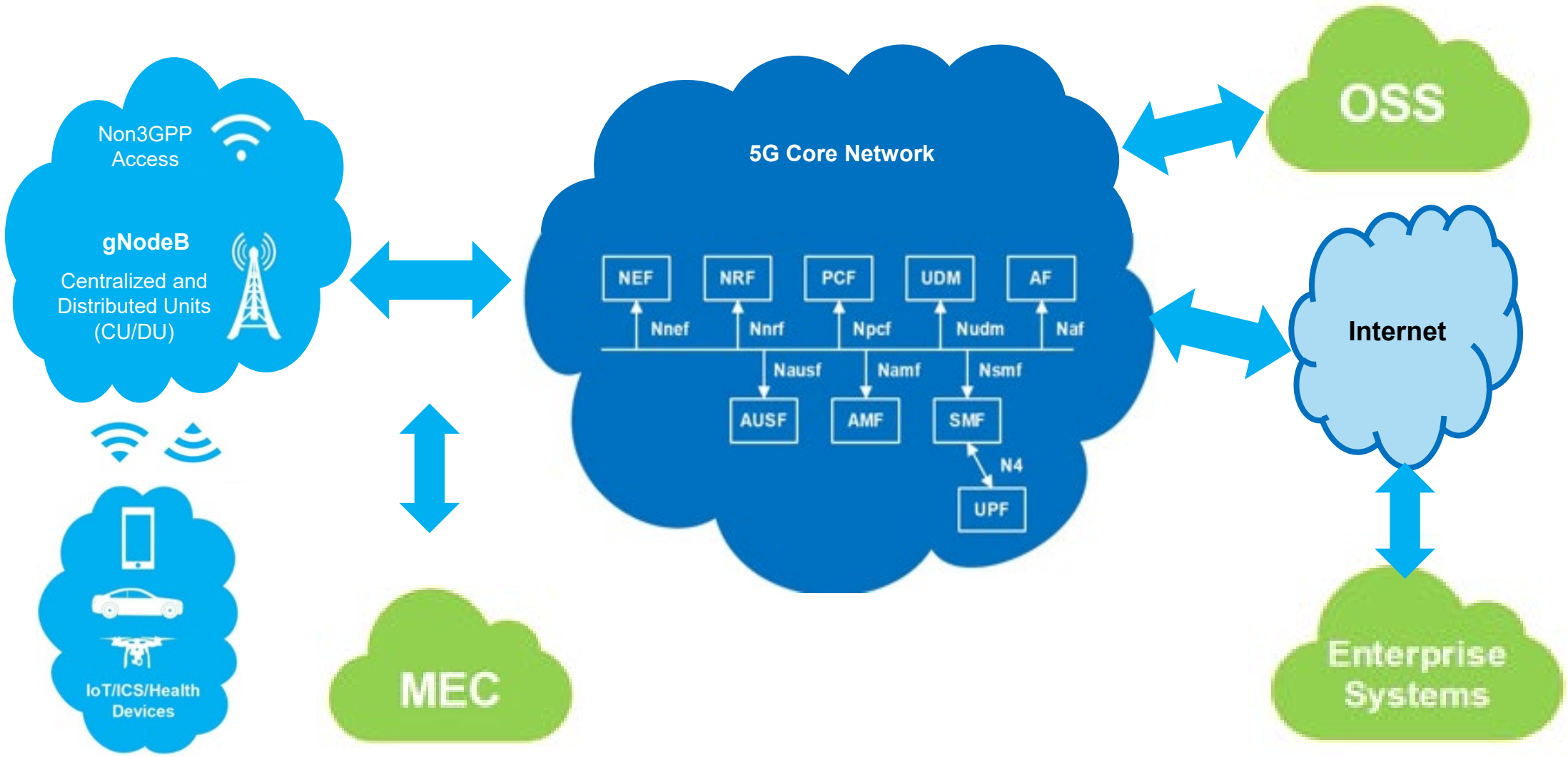
THE UNIVERSITY OF UTAH®

5G is a transformational technology

Courtesy of Kabir Kasargod, Qualcomm

Courtesy of Kabir Kasargod, Qualcomm

Simplified 5G Stand Alone (SA) Network Diagram



IoT: Internet of Things
ICS: Industrial Control System

MEC: Multi-access Edge Computing

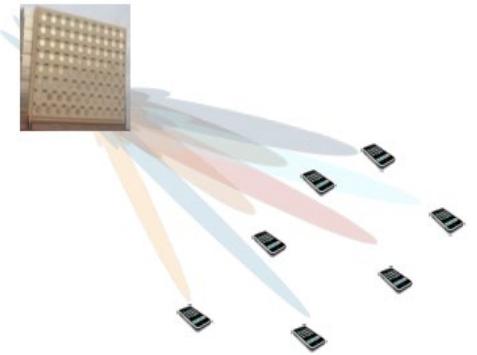
SDN: Software Defined Networking
NFV: Network Function Virtualization
OSS: Operational Support System

5G Spectrum – FCC Allocations

High-band (mmWave):

- ✓ 24 GHz, 28 GHz, upper 37 GHz (shared) , 39 GHz, and 47 GHz bands – total of about 5 GHz licensed
- ✓ **Unlicensed**: 64-71 GHz: 7 GHz of new unlicensed spectrum, doubles existing 47-64 GHz band

From 3GPP 5G Implementation Guidelines, GSMA



Medium-band: 2.5 GHz, 3.3-3.45 GHz (shared with airborne radar), 3.45-3.55 GHz, 3.55-3.65 GHz (shared by CBRS PAL and GAA users), and 3.7-3.98 GHz/C Band, 5.905-5.925 GHz (C-V2X)

- ✓ **Unlicensed**: 5.925-7.125 GHz, 1200 MHz at 6 GHz (Wi Fi 6E, 5G-NR-U).

From https://www.androidauthority.com/what-is-5g-mmwave-933631/

Private 5G Networks for Avionics

NR-U: New Radio in the Unlicensed Band, R16

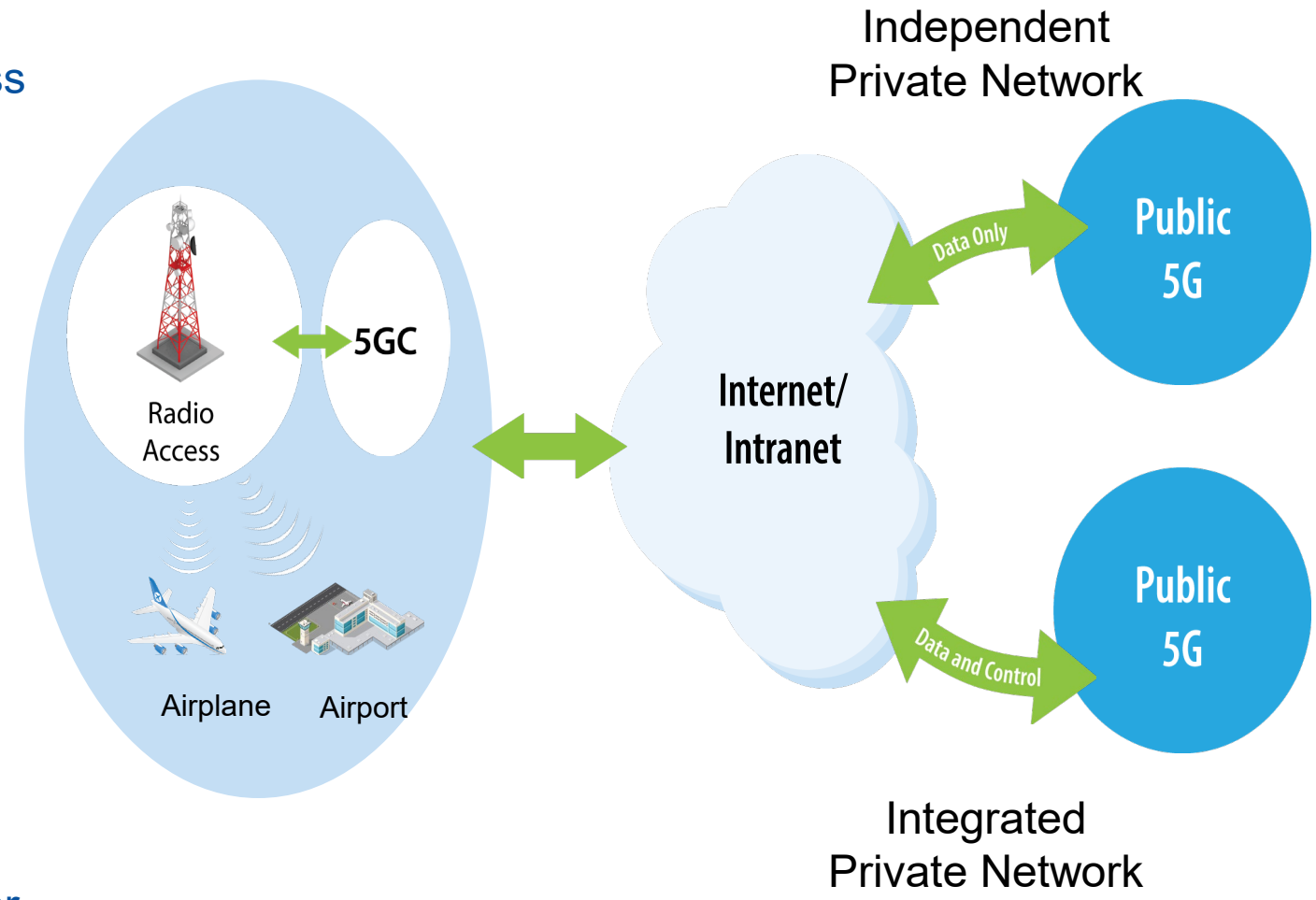
- ✓ Transformation of LTE Licensed Assisted Access (LAA)
- ✓ Standalone mode with **no licensed spectrum**

Network Configurations

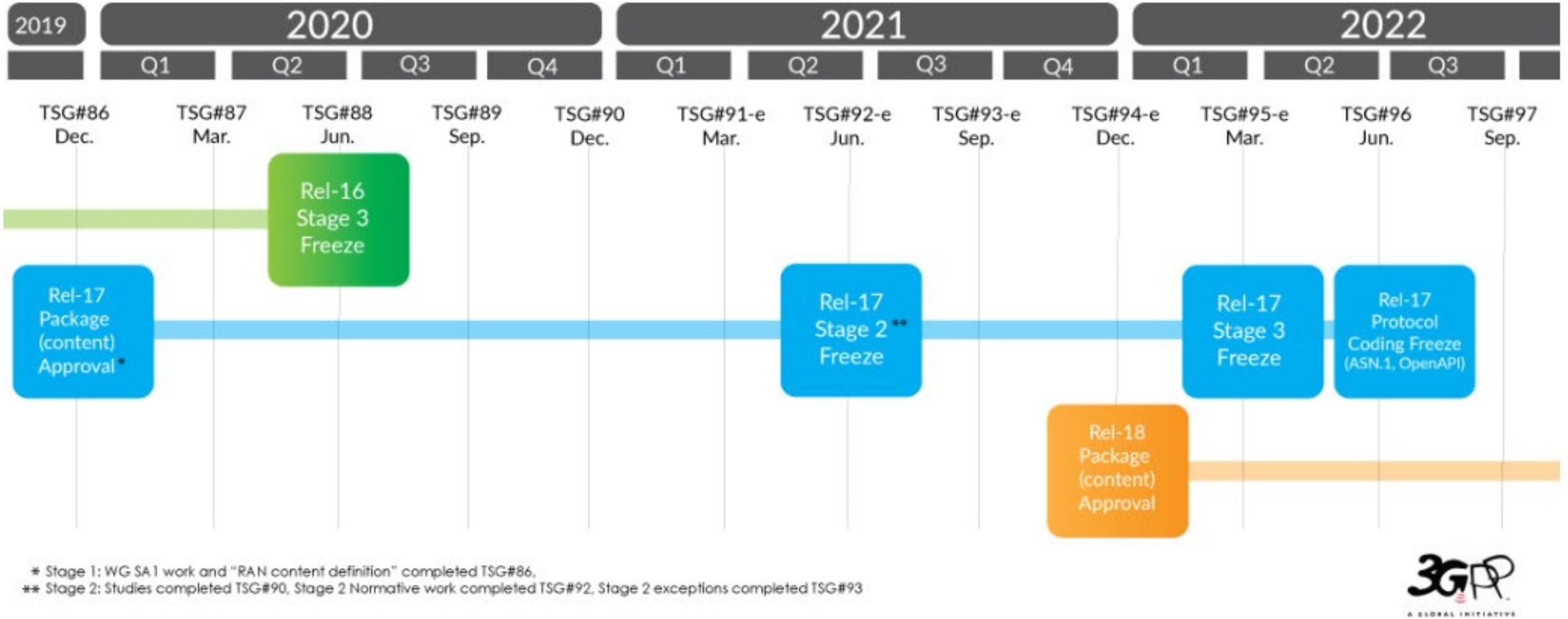
- ✓ Isolated and Independent
- ✓ Hybrid - Integrated with public network

Use cases:

- ✓ CBRS at Dallas Love Field Airport
- ✓ Manufacturing - Industry 4.0
- ✓ Smart Warehouse – DoD 5G Use Case
- ✓ Other use cases: Hospitals, Smart Grid, Nuclear Plants, Mines …..



5G Standards Timeline



* Stage 1: WG SA1 work and "RAN content definition" completed TSG#86.
** Stage 2: Studies completed TSG#90, Stage 2 Normative work completed TSG#92, Stage 2 exceptions completed TSG#93

Non-Terrestrial 5G in R16/R17

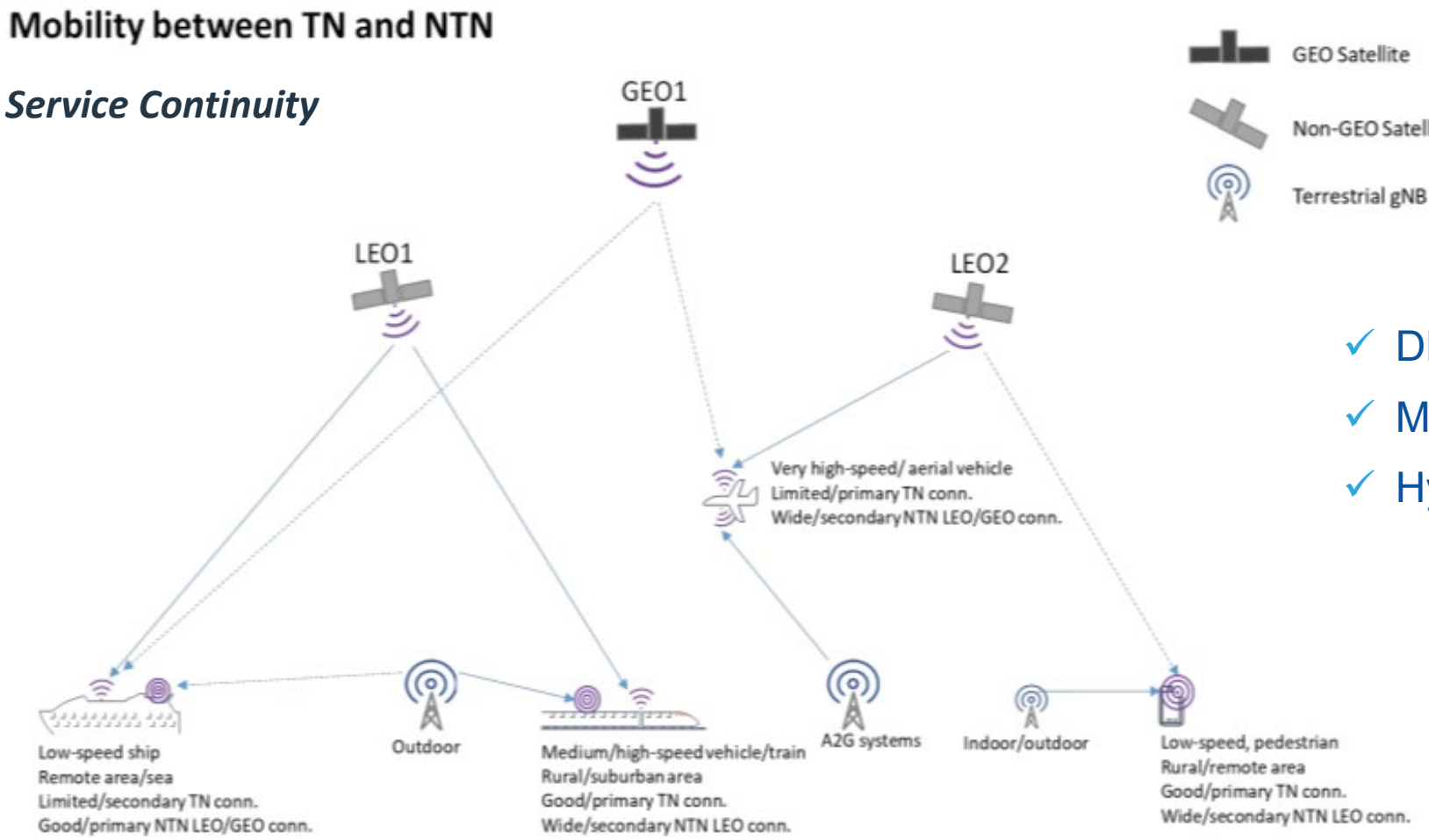


Figure 5.4-1: Typical example of NTN-TN interworking

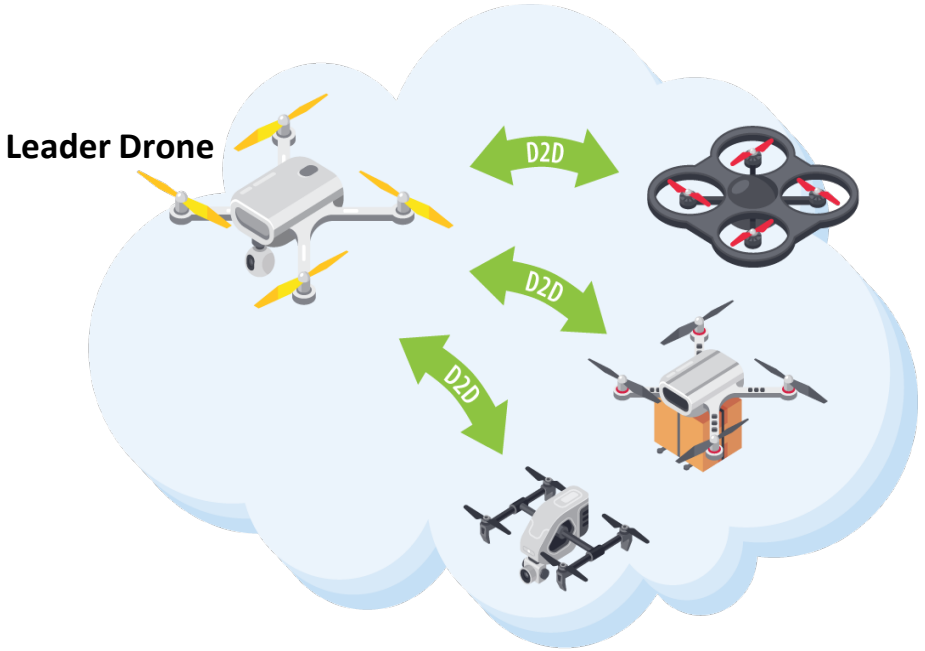
From 3GPP TR 38.821 V16.1.0

- ✓ DL 360 Mbps, UL 180 Mbps
- ✓ Mobility: 1000 km/h (621 mph)
- ✓ Hybrid - Integrated with public network

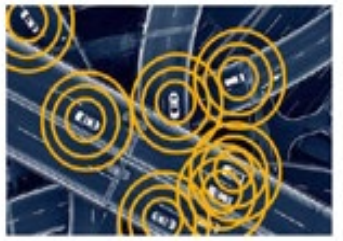
5G Side link: Device to Device (D2D) in R17

No-Coverage

No-Coverage



Swarm of Drones
(Group of Vehicles, Medical Equipment)



Extended sensing

Passing on environment data to other vehicles who are not within sensor distance

Platooning

Forming groups dynamically and reducing vehicle distance

5G New National Security Challenges

New key capabilities with 5G

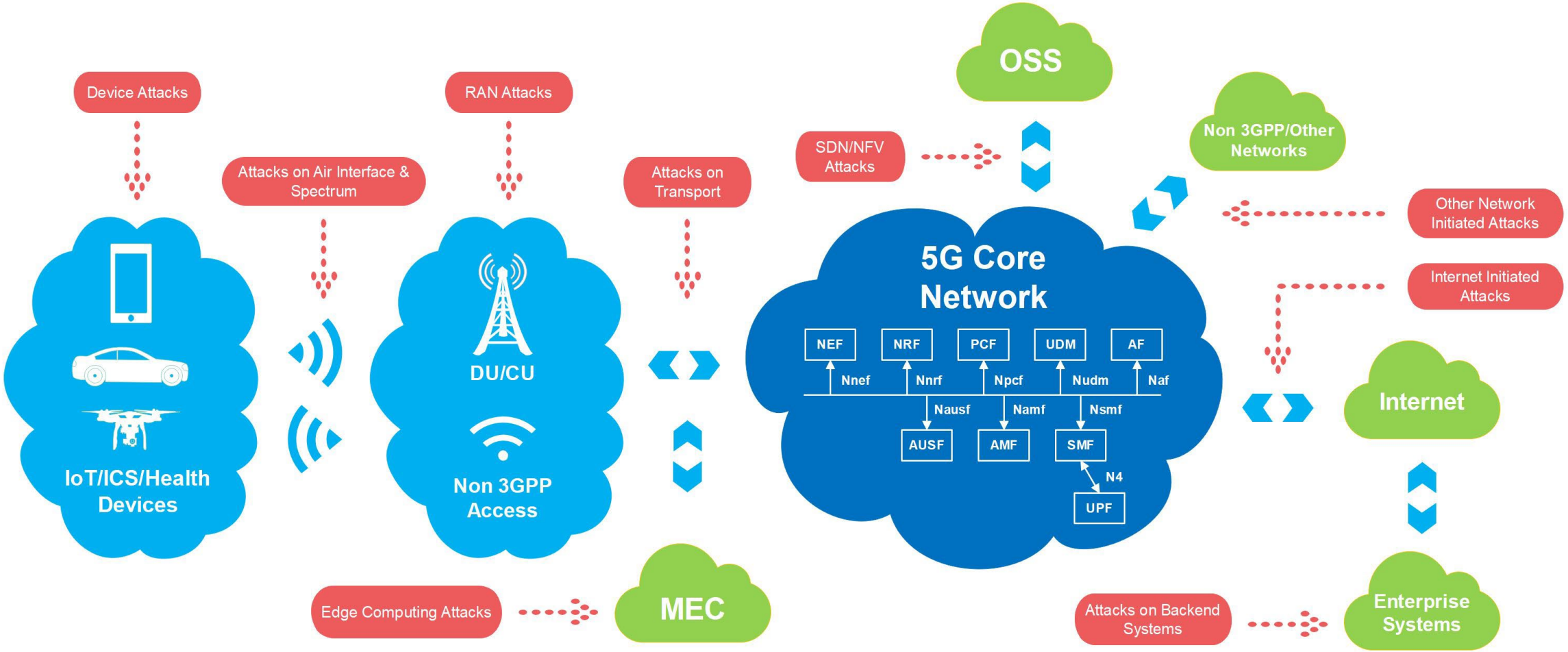
- 5G enabled IoT and industrial IoT, connected health, vehicles (V2X[1]), UAS/Drone (A2X[2]), etc.
- 5G Core (5GC) introduces Service Based Architecture (SBA)
- 5G NR (New Radio); use of unlicensed and shared spectrum
- Beam based Air Interface for sub-6 GHz and mmWave
- Edge computing, SDN[3] and NFV[4]

New Security Challenges

- Secure operation of large number of devices, vehicles, UAS/Drones; authentication and identification
- Increase in attack surface – need to secure increased number of interfaces
- Increase in illegal and disruptive use of spectrum sharing
- Adapting wireless security to beam based directional transmission, increase in mmWave base station density
- Secure operation of edge connectivity, SDN, and NFV

[1] Vehicle-to-Everything, [2] Aerial-to-Everything, [3] Software Defined Networking, [4] Network Function Virtualization

5G Network & Attack Surfaces



IoT: Internet of Things
ICS: Industrial Control System

MEC: Multi-access Edge Computing

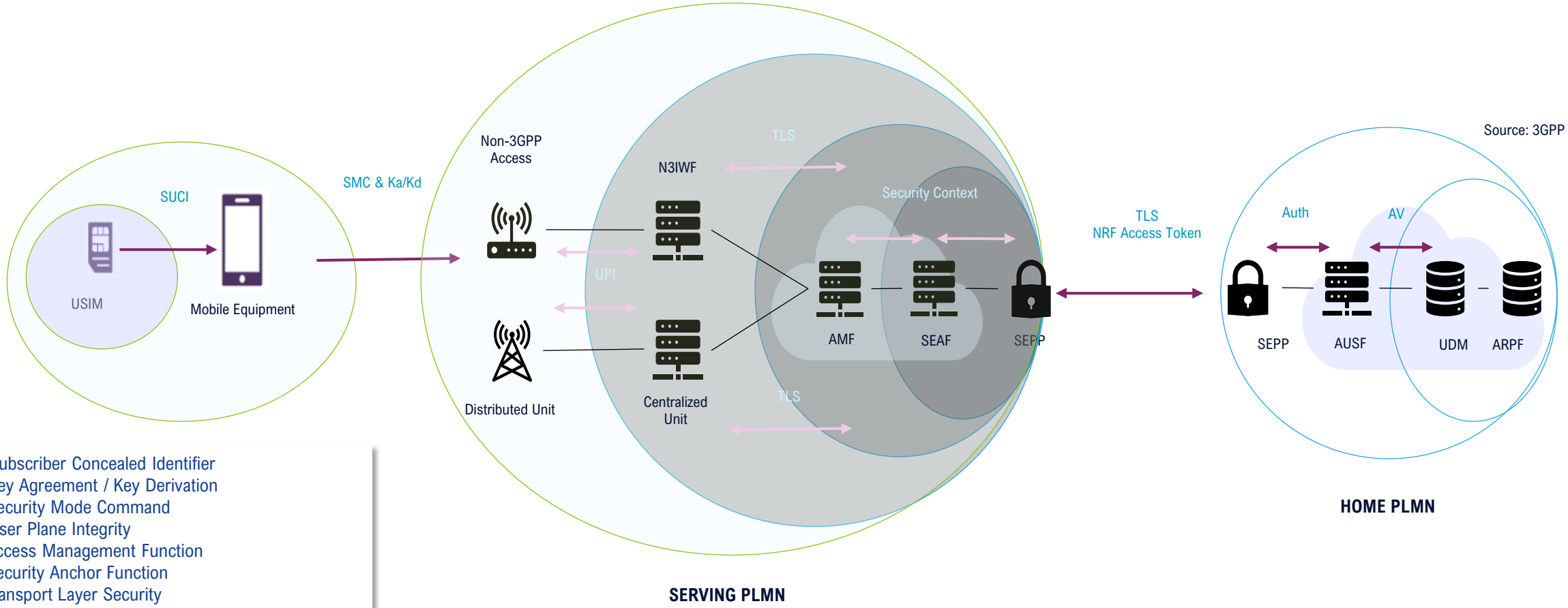
SDN: Software Defined Networking
NFV: Network Function Virtualization
OSS: Operational Support System

5G vs LTE Security: A short comparison

LTE Security	5G SA Security
UE Subscription identifier (IMSI) is exposed	Permanent Subscription Identifier (SUPI) is concealed over the air with Subscriber Concealed Identifier (SUCI)
No integrity protection of user data, packet injection is possible PDCP Transport layer	User-Integrity Protection
Core Network is based on point-to-point trusted interfaces	Service Based Architecture & TLS Mutual authentication (Zero trust framework)
Single authentication for network-attach	Primary and Secondary Authentication
HSS / HLR / AAA for multi-access authentication	Single Authentication Framework : AUSF (Authentication Server Function)
Roaming: No authentication confirmation to Home network	Authentication confirmation sent to the Home AUSF (Roaming)
Bid-down to GSM to Legacy	Security Mode Command & ABBA (Anti-Bidding down Between Architectures)

Reference: Nokia, 2020 Feb WSI Workshop

5G Security Trust Model (Includes Roaming)



SUCI Subscriber Concealed Identifier
Ka/Kd Key Agreement / Key Derivation
SMC Security Mode Command
UPI User Plane Integrity
AMF Access Management Function
SEAF Security Anchor Function
TLS Transport Layer Security
SEPP Security Edge Protection Proxy
Auth Authorization
AV Authentication Vector
UDM Unified Data Management
ARPF Authentication Credential Repository and Processing Function
NRF Network Repository Function
PLMN Public Land Mobile Network

Reference: Nokia, 2020 Feb WSI Workshop

Needed 5G Security for Mission Critical Communication

- Optional 3GPP security procedures*
  - ✓ User plane encryption
  - ✓ Integrity Protection for user data
- 5G Network Slicing for customized security policy
  - ✓ Secondary authentication
  - ✓ Authentication, Authorization and Accounting Server (AAA-S)
- 5G Network Configurations
  - Certificate management
  - Null encryption scheme
- ML based solutions for detection and mitigation of attacks
- Application layer solutions – Security Apps

* Reference: CSRIC Report on RECOMMENDATIONS FOR IDENTIFYING OPTIONAL SECURITY FEATURES THAT CAN DIMINISH THE EFFECTIVENESS OF 5G SECURITY

Idaho National Laboratory