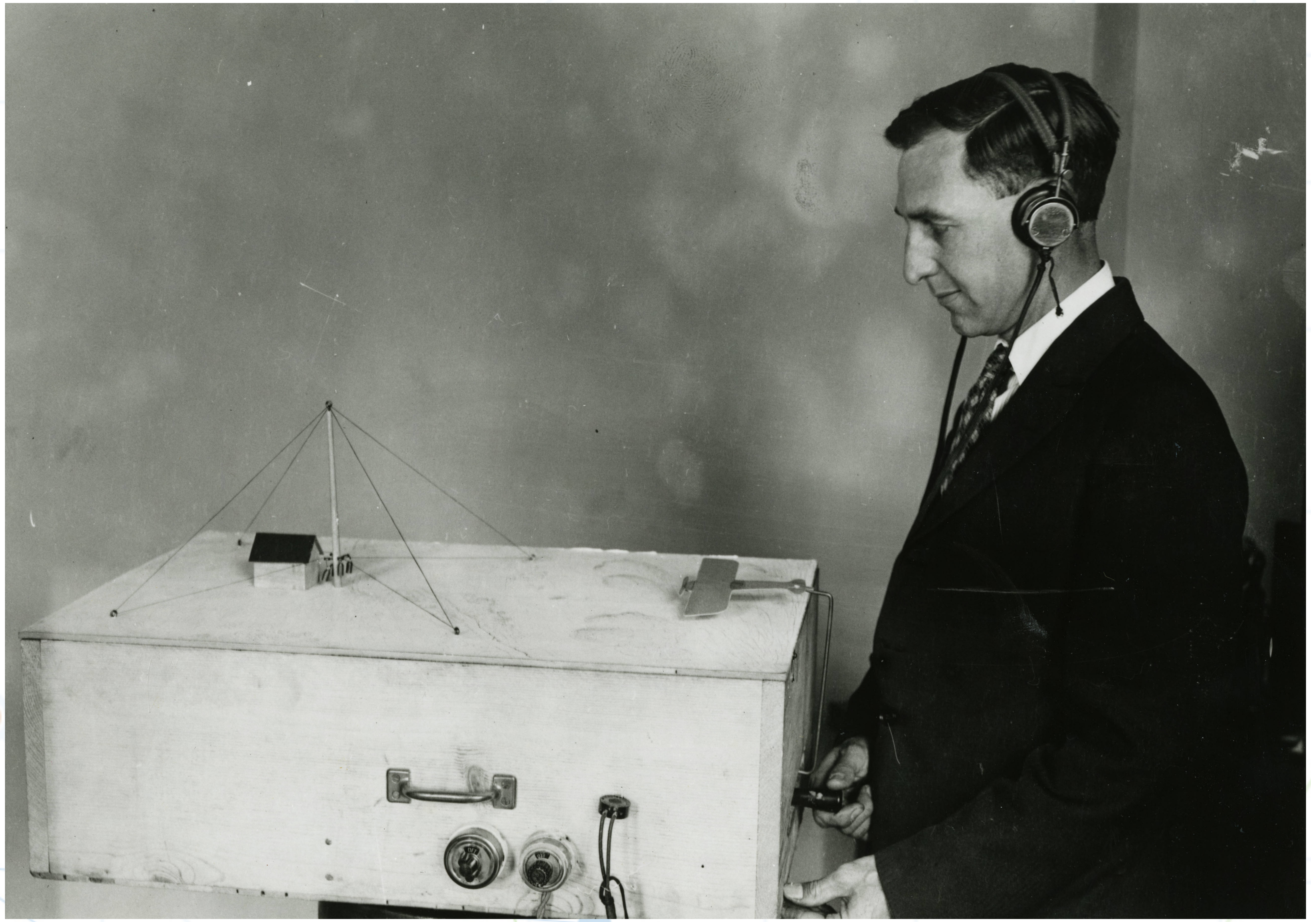


NIST Activity in 5G and Beyond Security

Jeff Cichonski

and

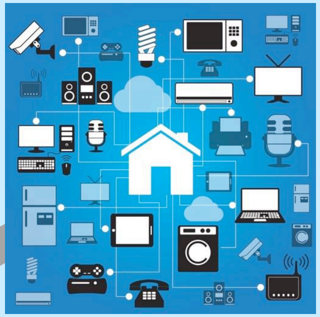
Nada Golmie

National Institute of Standards and Technology
U.S. Department of Commerce

What is 5G?

Improved Communications Capabilities

Use Cases



Different demand, size, complexity

Connectivity

Users, Infrastructures,Things
Cellular, Vehicular, Drones,
Direct, Hotspot

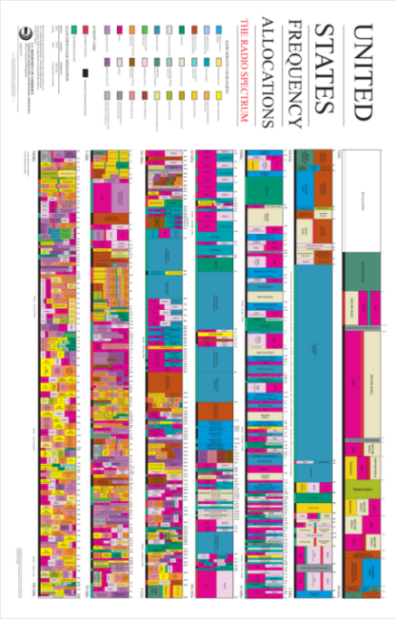
Adaptability

Autonomous Resilient
Low overhead
Environment aware

High Capacity

Modulation schemes
Multiple Antennas
mmWave bands
Network densification

Efficient Spectrum Utilization



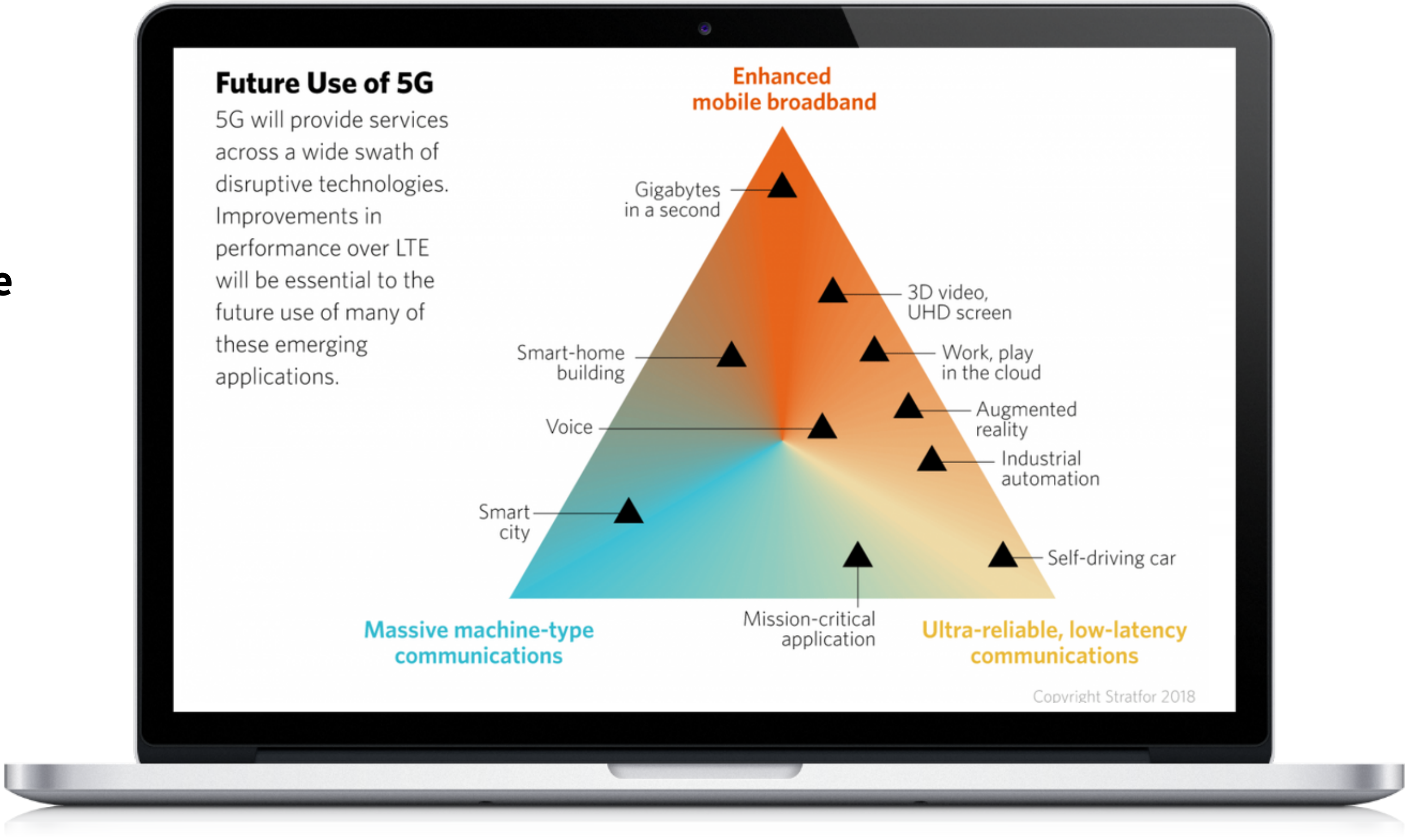
The 5G Capabilities

High Speed

Massive IoT

Low Latency Ultra-Reliable

5G has been envisioned and designed to provide capabilities focused on three core use cases.

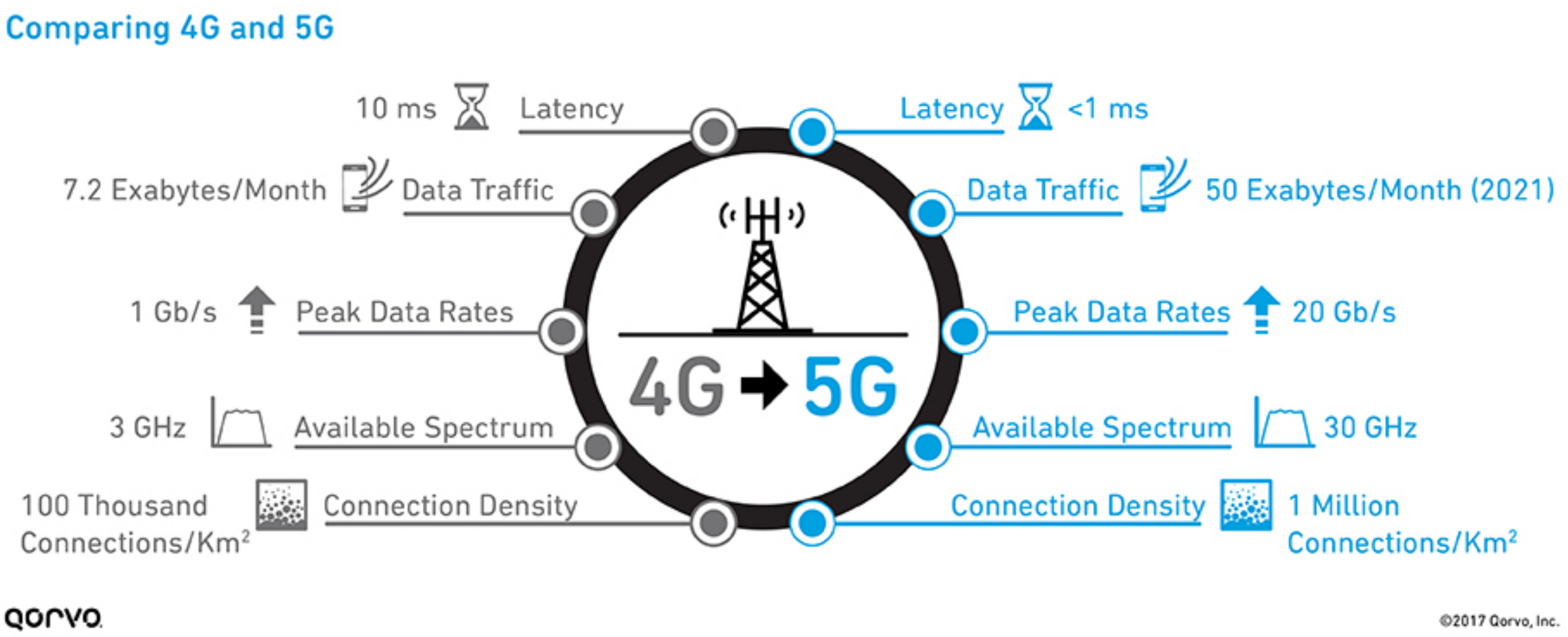


Future Use of 5G

5G will provide services across a wide swath of disruptive technologies. Improvements in performance over LTE will be essential to the future use of many of these emerging applications.

Copyright Stratfor 2018

4G to 5G



Comparing 4G and 5G

10 ms Latency

7.2 Exabytes/Month Data Traffic

1 Gb/s Peak Data Rates

3 GHz Available Spectrum

100 Thousand Connections/Km^2 Connection Density

Latency <1 ms

Data Traffic 50 Exabytes/Month (2021)

Peak Data Rates 20 Gb/s

Available Spectrum 30 GHz

Connection Density 1 Million Connections/Km^2

qorvo

Foundational Standards Organizations

Insert Your Subtitle Here

Internet Engineering Task Force

Internet Protocols

- TCP/IP, TLS, IPSEC

3rd Generation Partnership Program

Cellular Systems

- 3G, LTE, VOLTE, 5G

European Telecommunications Standards Institute

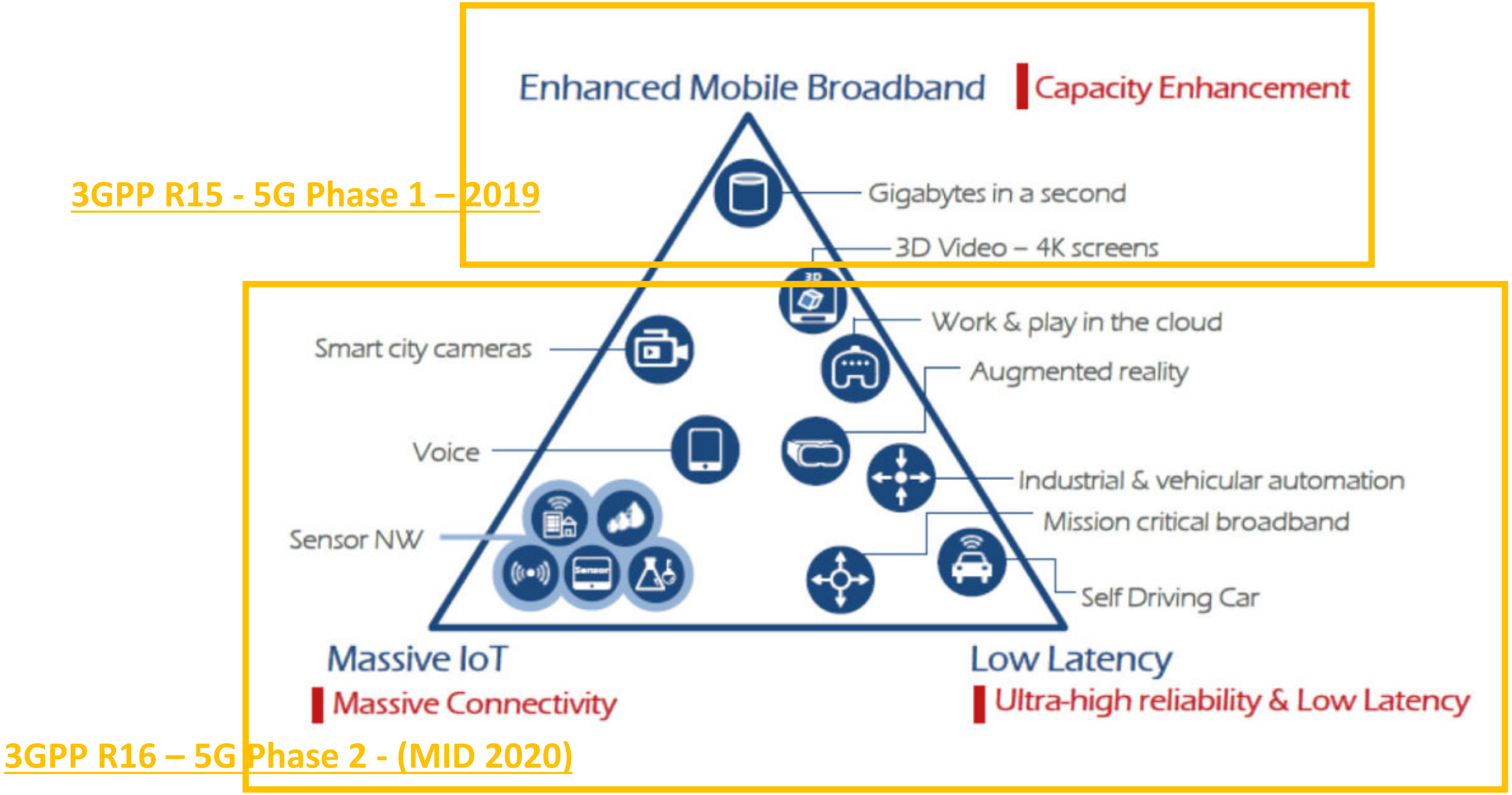
Virtualization Standards

ICT Standards

Institute of Electrical and Electronics Engineers

802.11 - WiFi

3GPP Perspective: 5G *New Radio*



3GPP R15 - 5G Phase 1 – 2019

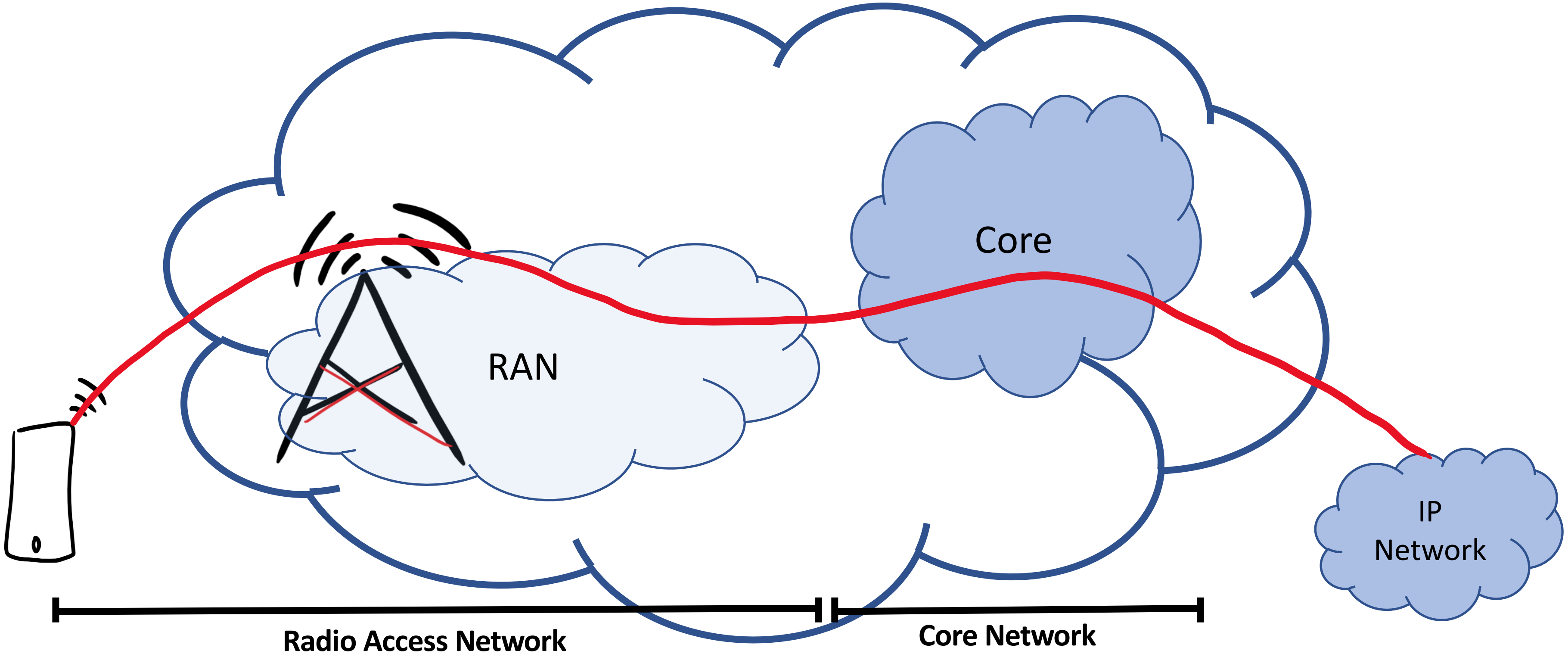
3GPP R16 – 5G Phase 2 - (MID 2020)

Source: ITU-R-M-2083

3GPP Working Groups

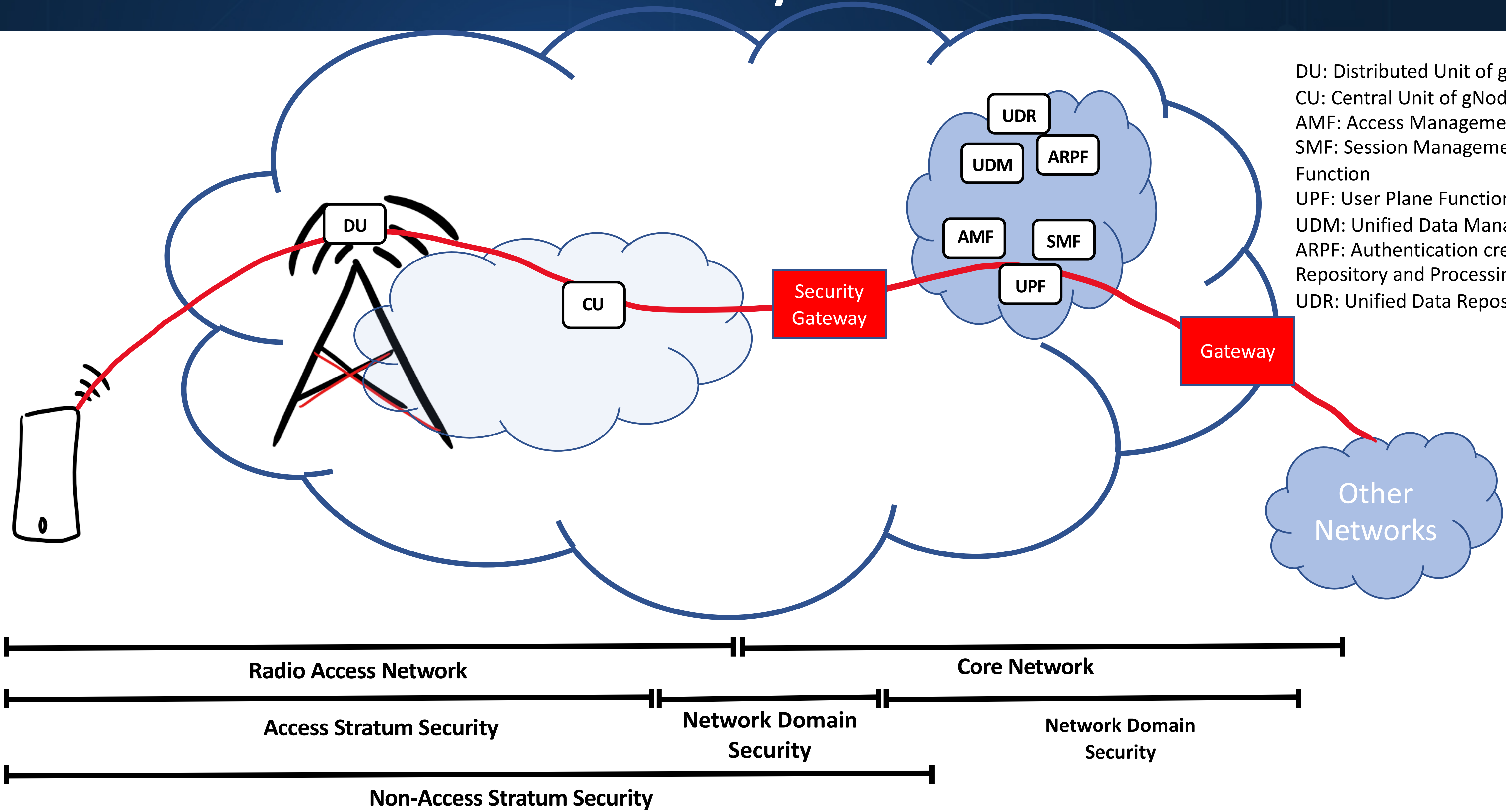
Radio Access Network (RAN)	Service & Systems Aspects (SA)	Core Network & Terminals (CT)
RAN 1 - Radio Layer 1 (Physical)	**SA 1 - Services**	**CT 1 – User equipment & Core network radio protocols**
RAN 2 - Radio Interface architecture and protocols	SA 2 - Architecture	CT 3 - Interworking between a 3GPP networks and external nodes or networks
RAN 3 - Radio architecture and Interface protocols	**SA 3 - Security**	CT 4 – Core network aspects
RAN 4 - Radio performance and protocol aspects	SA 4 - Codec	CT 6 – Smart card application aspects (SIMS)
RAN 5- Mobile terminal conformance testing	SA 5 - Telecom Management	
	SA 6 – Mission Critical	

Mobile Network – The Basics



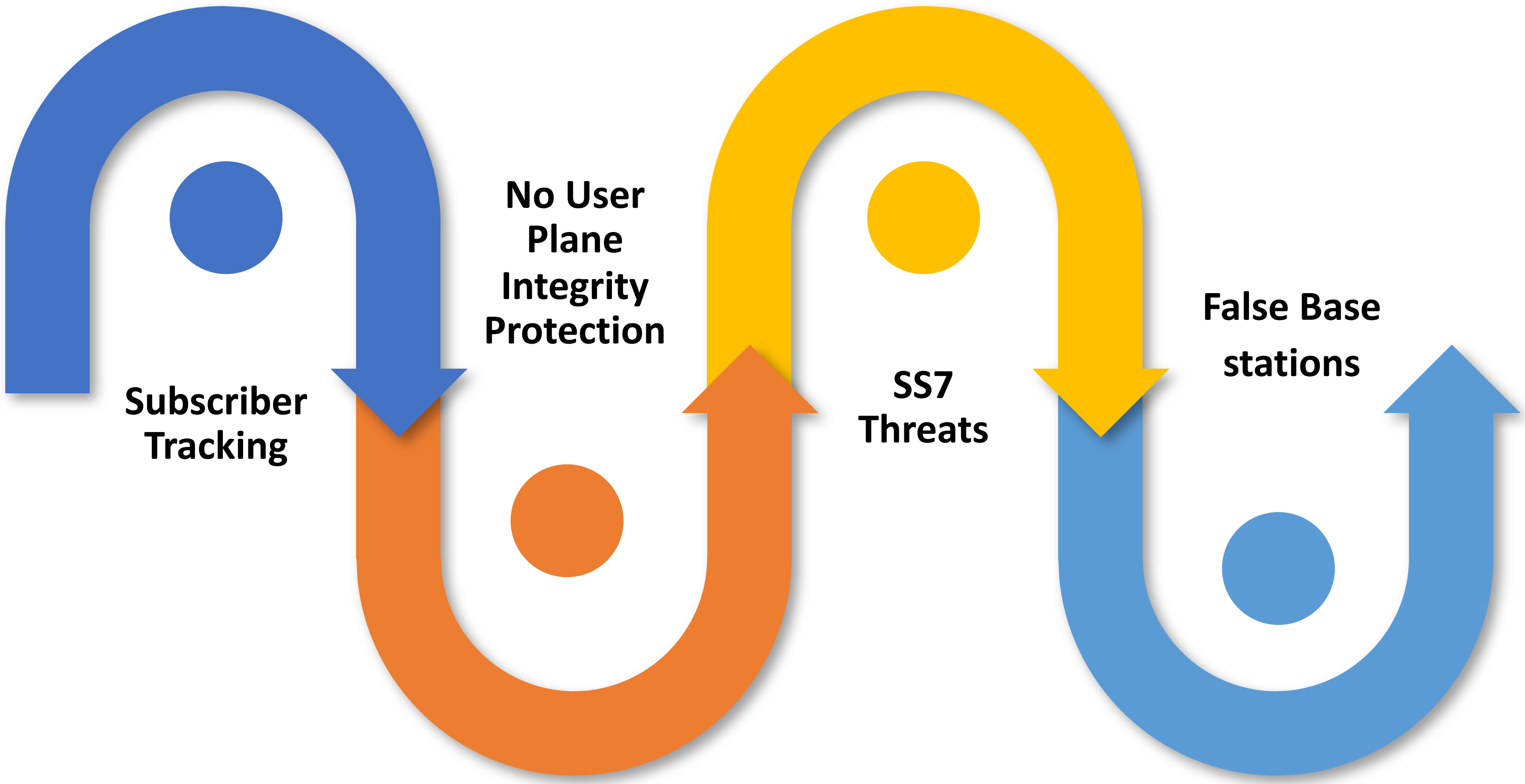
- A device connects to a network of base stations or Radio Access Network (RAN)
- The RAN connects to a 3GPP Packet Core (Core)
- The Packet Core provides connectivity to the internet or other IP network.

Mobile Network Security in a Nutshell



DU: Distributed Unit of gNodeB
CU: Central Unit of gNodeB
AMF: Access Management Function
SMF: Session Management Function
UPF: User Plane Function
UDM: Unified Data Management
ARPF: Authentication credential Repository and Processing Function
UDR: Unified Data Repository

Known Security Issues With LTE



Subscriber Tracking

No User Plane Integrity Protection

SS7 Threats

False Base stations

Security Enhancements

Radio Network Security

Subscriber Privacy

Roaming Security

Increased Visibility

Network Slicing

Authentication Enhancments

5G Cybersecurity at the National Cybersecurity Center of Excellence

Enhanced Security Capabilities

Demonstrate increased cybersecurity protections in 5G networks from the addition of standards-based features

Modern Supporting Technologies

Increased use of modern information technologies Supporting the 5G System to allow for the addition of modern cybersecurity best practices

Practical Approach

As 5G technologies are still being specified and developed it’s important to effectively scope and prioritize this effort

Focused Security Capabilities

1 Trusted Hardware

Compute hardware will provide the capability to measure platform components and store the measurements in a hardware root of trust for later attestation. NFs will run on top of this trusted hardware

2 Isolation and Policy Enforcement

Technically enforce policies that define which servers in the compute environment NF's can run on, based on trust values and asset tags. The platform trust measurement and asset tagging can also be used as part of the data protection policy of the NF's

3 3GPP Security Feature Enablement

Configured in accordance with recommended industry practices, including enabling standards-based security features and configuring parameters in accordance with relevant guidelines

4 False Base Station Protections

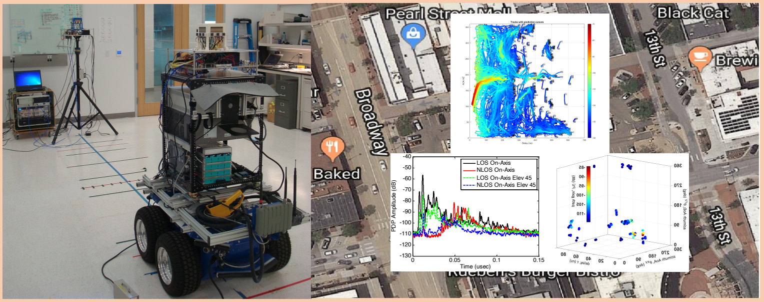
Utilize commercial solutions to mitigate and provide protections from false base stations that are not provided by the 3GPP standards. Including potentially configuring the network to disable legacy RATs on the UE

NIST’s Efforts Related to 5G

Advances in Communications Metrology

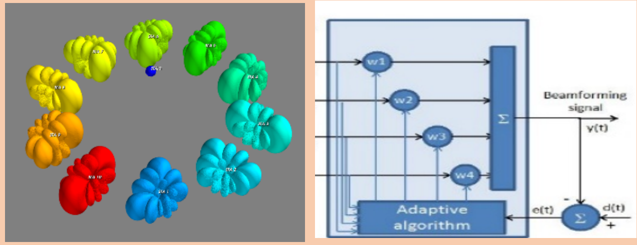
Public Safety Communications Research

Advanced Manufacturing

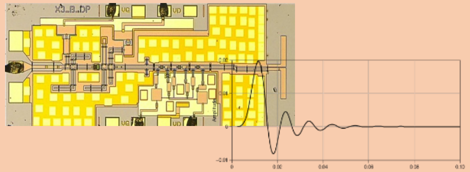


Channel propagation measurement and modeling, standards development

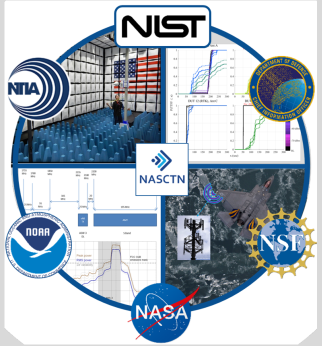
Antenna Meas. Facility
MIMO Antenna Testing



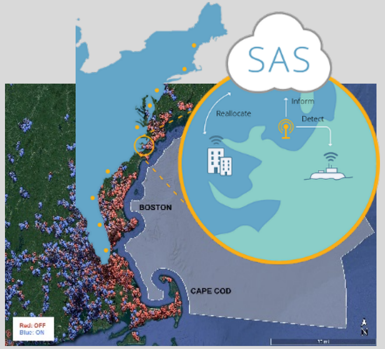
Beamforming modeling and system level performance evaluation



mmWave measurement
Signal characterization



Trusted spectrum testing



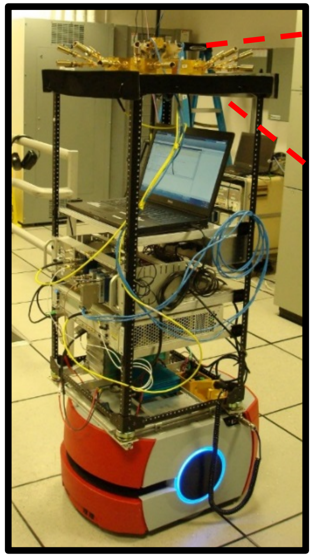
Spectrum sharing measurement and modeling, standard development

Security of advanced communications technologies & applications

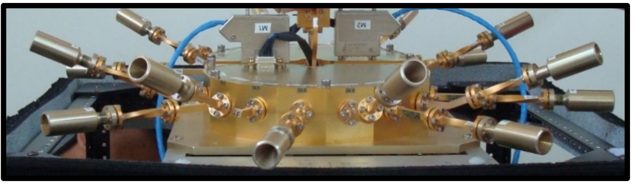
NIST mmWave Measurement & Modeling Capabilities

Channel Sounders for 83.5, 28, and 60 GHz

TX ARRAY



RX ARRAY

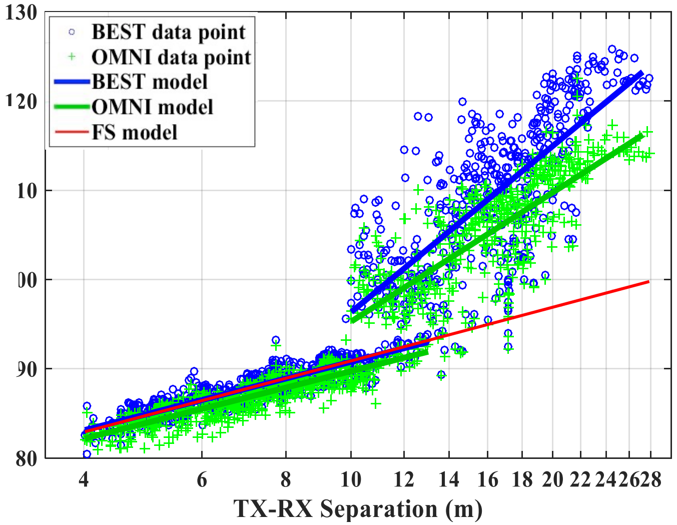


Zoom RX Array

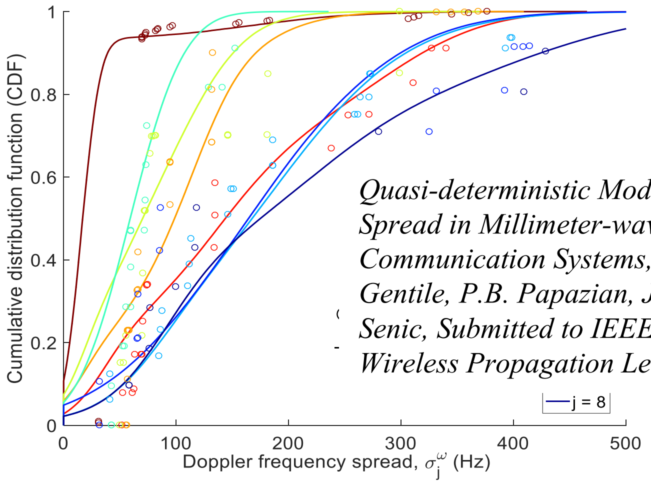
P.B. Papazian, C. Gentile, K.A. Remley, J. Senic, J.-K. Choi, N. Golmie "A Radio Channel Sounder for Mobile Millimeter-Wave Communications: System Implementation and Measurement Assessment," IEEE Trans. on Microwave Theory and Techniques, vol. 64, no. 9, pp. 2924-2932, Sept. 2016.

Path Loss

"Pathloss Models for Indoor Hotspot Deployment at 83.5GHz," C. Gentile, J. Senic, P. Papazian, J-K. Choi, K. Remley, IEEE Globecom 2016.

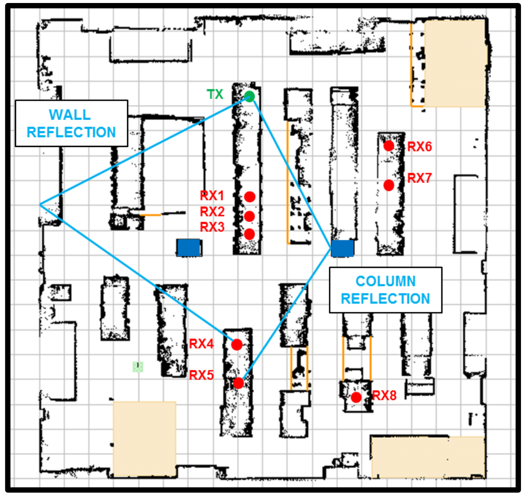


Doppler Spread

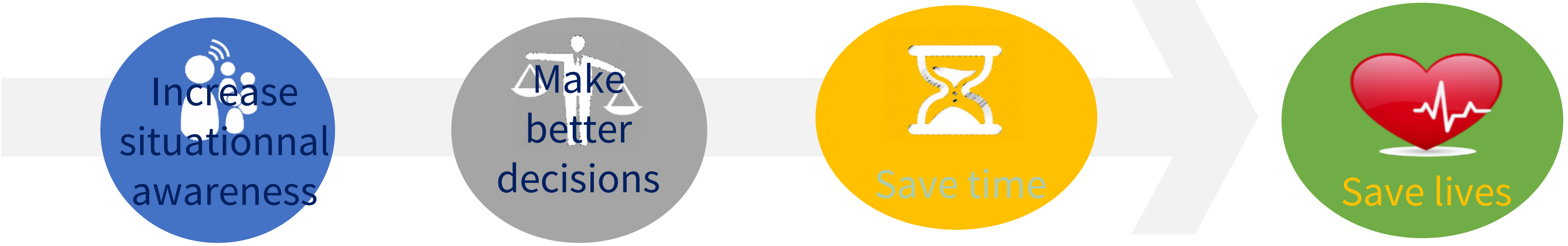


Quasi-deterministic Model for Doppler Spread in Millimeter-wave Communication Systems," J. Wang, C. Gentile, P.B. Papazian, J.-K. Choi, J. Senic, Submitted to IEEE Antennas and Wireless Propagation Letters.

Map-Based Dispersion Models



5G for Public Safety Communications



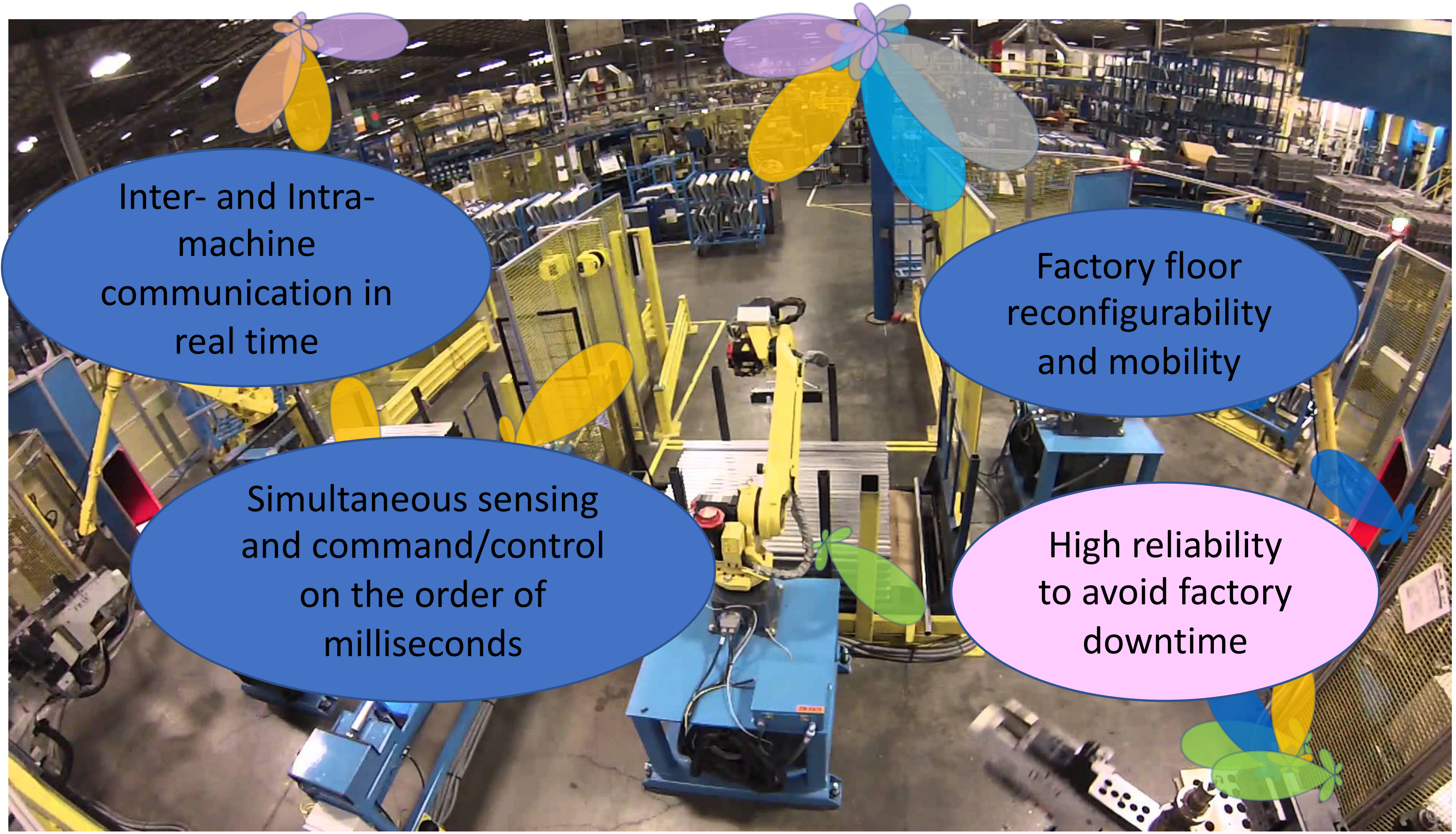
Increase situationnal awareness

Make better decisions

Save time

Save lives

5G for Smart Manufacturing


Inter- and Intra-machine communication in real time
Factory floor reconfigurability and mobility
Simultaneous sensing and command/control on the order of milliseconds
High reliability to avoid factory downtime

The Enablers:

New wireless technologies => breakthroughs in manufacturing

The Challenges:

- Harsh wireless-channel conditions
- Stringent communication requirements:
  - Low latency (fast)
  - High reliability
  - Scalable: few or many nodes

5G mmWave Channel Model Alliance

NIST

- Established user community: https://sites.google.com/a/corneralliance.com/5g-mmwave-channel-model-alliance-wiki/home

- Repository of data measurements and models available online: https://5gmm.nist.gov/

- Sponsored workshops and face-to-face meetings co-located with major conferences & events: IEEE ICC, VTC, GLOBECOM, NSF mmWave Research Coordination Network, others.

80
Organizations Represented

Academia

1. Beijing Jiaotong University
2. Boise State University
3. Carleton University (Canada)
4. Florida International University
5. Fraunhofer Institute
6. Georgia Institute of Technology
7. Indian Institute of Science
8. ITRI (Taiwan)
9. Michigan Technological University
10. Missouri S&T
11. Morgan State University
12. National Institute of Technology (India)
13. New Jersey Institute of Technology
14. New York University Wireless
15. North Carolina State University
16. Pennsylvania State University
17. Polytechnic University of Leiria (Portugal)
18. Portland State University
19. Princeton
20. Stanford University
21. Stevens Institute of Technology
22. Technische Universität Dresden
23. Technische Universität Ilmenau
24. Tufts University
25. UC Santa Barbara
26. University at Buffalo
27. University of British Columbia
28. University of California, Berkeley
29. University of California, Irvine
30. University of California, San Diego
31. University of California, Santa Barbara
32. University of Chicago
33. University of Colorado, Boulder
34. University of Durham (UK)
35. University of New Mexico
36. University of South Carolina
37. University of Southern California
38. University of Texas
39. University of Vermont
40. University of Wisconsin
41. Universita Degli Studi Di Padova

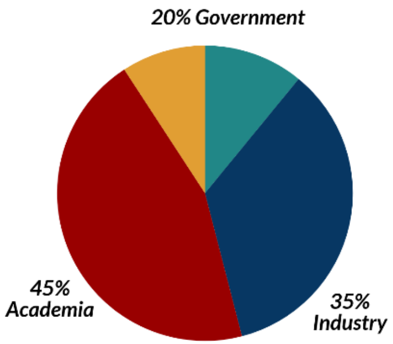
Government

42. DARPA
43. Defense Spectrum Organization
44. ETRI (South Korea)
45. Federal Communications Commission
46. National Institute of Metrology, China
47. National Science Foundation
48. NIST
49. NTIA
50. US Navy
51. Communications Research Centre (CA)

Industry

52. Alcatel-Lucent
53. Anritsu
54. AT&T
55. Azimuth Systems
56. Ball Aerospace
57. Cable Labs
58. Dow
59. DuPont
60. Echostar
61. Facebook
62. Forsk
63. Huawei Technologies
64. Huawei Technologies Canada
65. IEEE
66. Intel
67. InterDigital
68. Keysight
69. National Instruments
70. Nokia
71. octoScope
72. Qualcomm
73. Rohde & Schwarz
74. RT Logic
75. Samsung
76. Siradel
77. SK Telecom
78. Spirent
79. Sporton International
80. Xilinx

Contact Marc Leh (mleh@corneralliance.com) for more information



5G Alliance Deliverables include:

Measurement & Modeling White Papers

5G Alliance Data Repository

Measurement Verification Program

Channel Modeling Refinement

Measurement Campaign Support

Scenario & Parameter Description

Contact: Nada Golmie, nada.golmie@nist.gov

5G Collaborations

- **NCCoE 5G Security:** Collaboration with industry to demonstrate how the commercial grade components of 5G architectures can be used to enable cutting edge security features.
- **Documentary standard development**: 3GPP, IETF, IEEE, ANSI, Wireless Innovation Forum Spectrum Sharing Committee, CTIA, Telecom Infra Project.
- **Partnerships** across government, industry, academia.
- Public safety innovation accelerator program: 150 partnerships through ***prize challenges***, ***grant*** and ***cooperative agreements***.

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

5G Millimeter Wave Channel Model Alliance