INL/CON-22-67504-Revision-0

Idaho National Laboratory (INL) Wireless Test Beds for Over the Air (OTA) experimentation

June 2022

Arupjyoti Bhuyan

Changing the World's Energy Future

Idaho National Laboratory

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

INL/CON-22-67504-Revision-0

Idaho National Laboratory (INL) Wireless Test Beds for Over the Air (OTA) experimentation

Arupjyoti Bhuyan

June 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)

June 1, 2022

INL Wireless Test Beds for Over the Air (OTA) Experimentation

Idaho National Laboratory

INL Wireless Security Institute (WSI)

VISION

Advance 5G National Leadership and Accelerate the Secure Adoption of 5G and Beyond Technology

MISSION

Provide best in class policy and decision data, security evaluation, engineering support, and technology development enabling government and industry to maximize the benefits of 5G and beyond technology

Wireless Security Applied R&D

Conduct R&D addressing critical national wireless security gaps

Spectrum Innovation

Conduct R&D on Dynamic Spectrum Access to solve spectrum sharing gaps

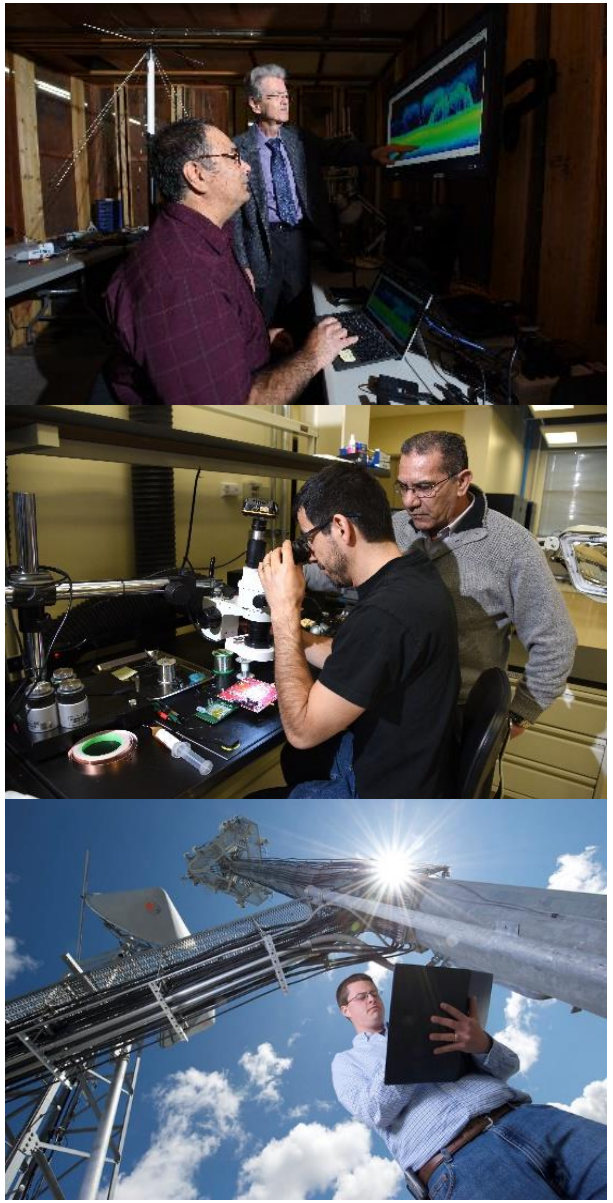
Next Generation Wireless Test Bed (WTB)

Effective, accurate, responsive testing at scale

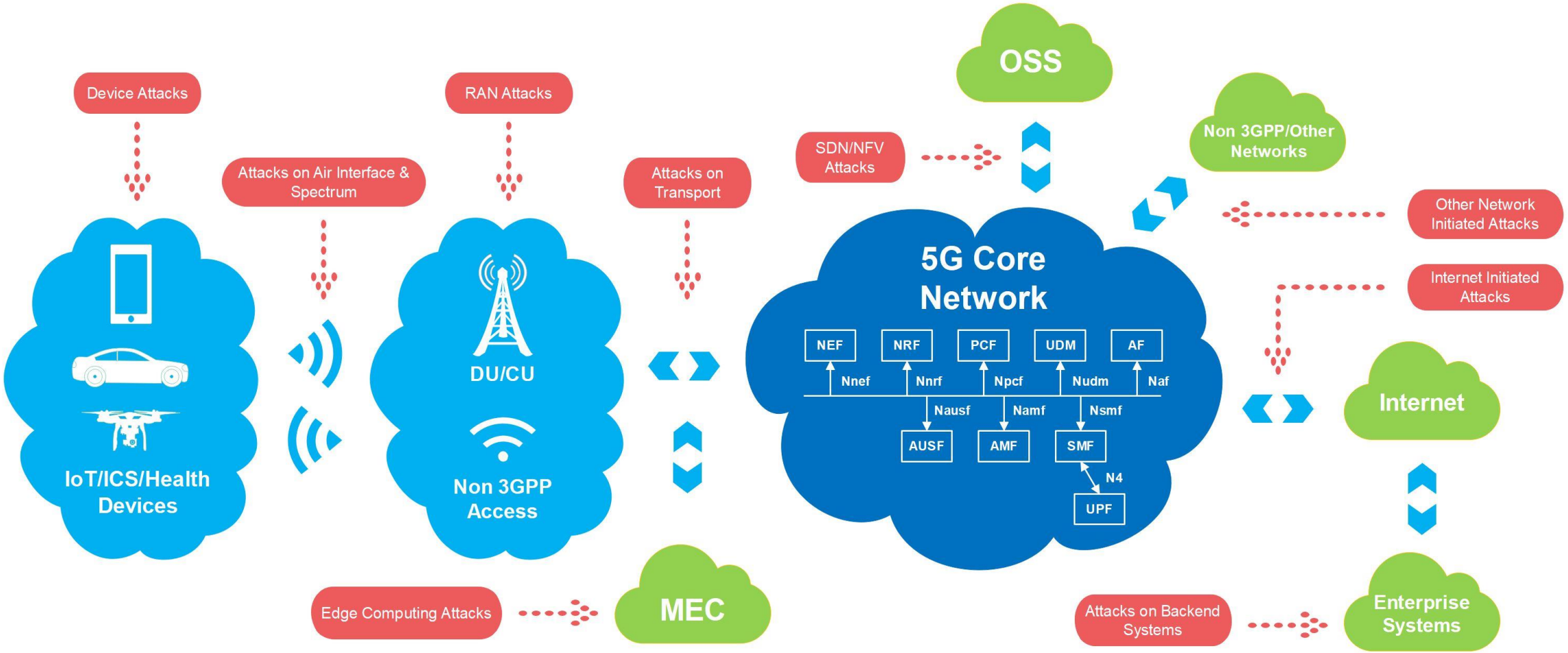
END STATE

Broad, Diversely Funded RDD&D Portfolio

INL Established as National Authority on Wireless Security



5G Network & Attack Surfaces



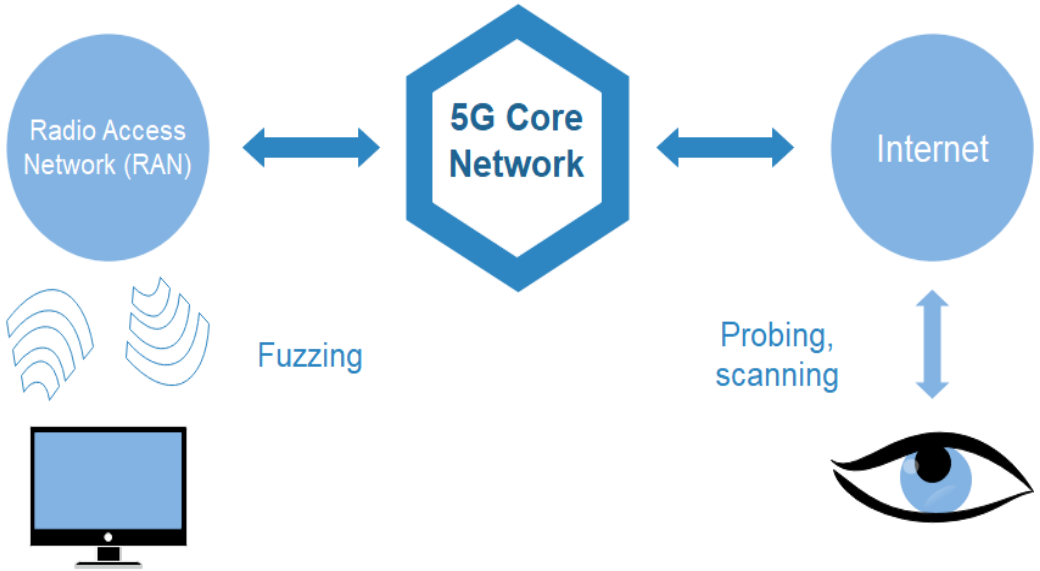
IoT: Internet of Things
ICS: Industrial Control System

MEC: Multi-access Edge Computing

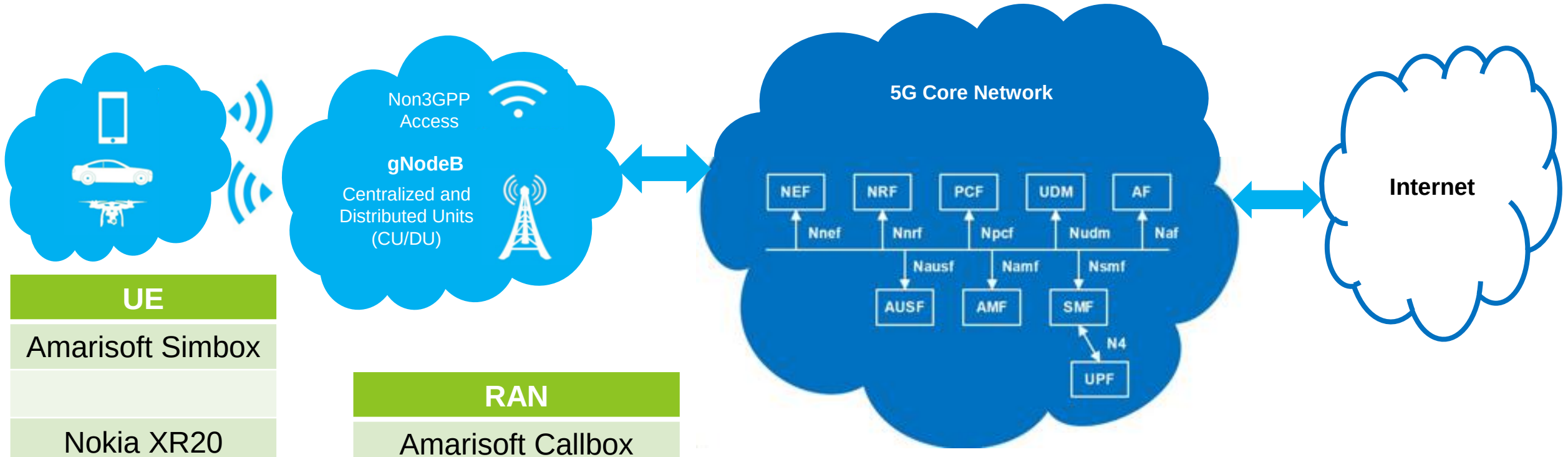
SDN: Software Defined Networking
NFV: Network Function Virtualization
OSS: Operational Support System

5G Security Assessment – Devices, RAN, and 5GC

- 3GPP 5G Security Properties/Requirements
  - ✓ Authentication
  - ✓ Privacy – User Identity, Data, and Location
  - ✓ Confidentiality, Integrity, Availability
- 5G Improvements
  - ✓ Encryption of identity, integrity protection for user data
  - ✓ Security policy through network slicing
- Risk Analysis with Adversarial Testing to assess a) Zero Trust Architecture and b) Defense in Depth
  - ✓ Threat scenarios
  - ✓ Network and device originated attacks



5G Standalone (SA) Laboratory Network



UE
Amarisoft Simbox
Nokia XR20
Samsung S21
Other 5G devices/handsets

RAN
Amarisoft Callbox
Nokia gNodeB
RadiSys gNodeB

5G Core
Free5GC
Open5GS
Open5GCore*

* planned

Unique National Security Infrastructure and Capabilities

Electric Grid Test Bed

Commercial Feeds,
Test Loops/Spurs

Water Security Test Bed

Municipal Water System

Radiological Ranges

First Responder Training

Specific Manufacturing

Quality Product

Wireless Test Bed

Agile Spectrum

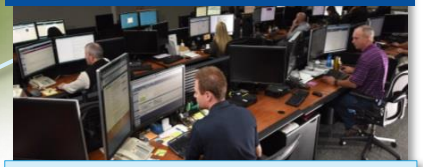
National Security Test Range

~20k TNT, VA Center

Nuclear Materials R&D

Electro-refining, SNM for Test/R&D

Research and Education Campus



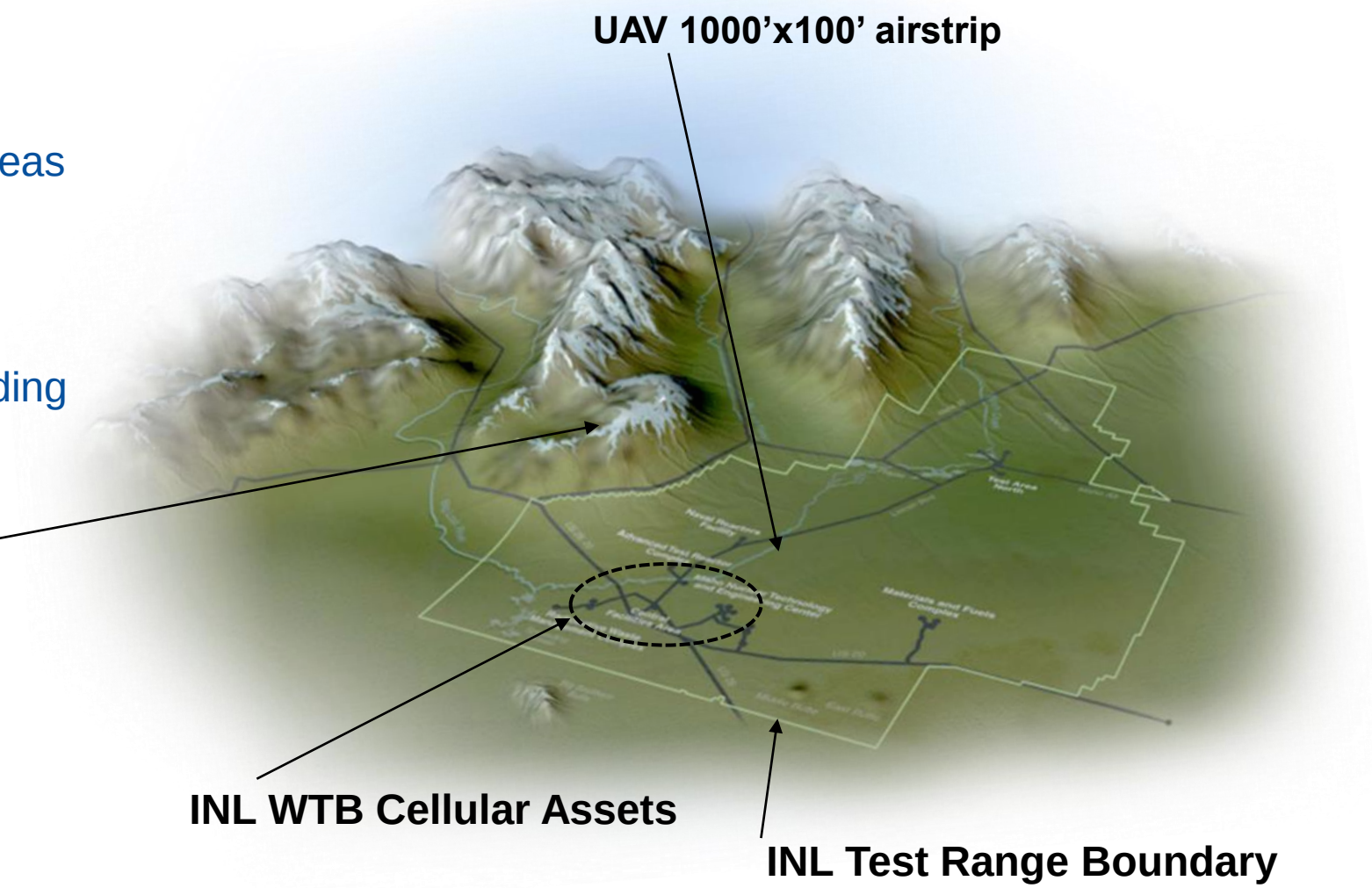
Controls & Energy Security Labs

- ✓ **Full-scale real-world testing and demonstrations for deployment** *(designed, built and operated by INL)*
- ✓ **Integrated testing across multidisciplinary areas** *(radiological, physical security, explosive, power, controls, cyber)*
- ✓ **Rapid development through model, test, validate, and refine** *(high fidelity, effects-based modeling, rapid testing and measurement)*
- ✓ **Access to the full range of support services** *(lineman, engineers, rad techs, fire fighters and security forces)*
- ✓ **Ability to develop prototypes, manufacturing process and resolve uncertainty**

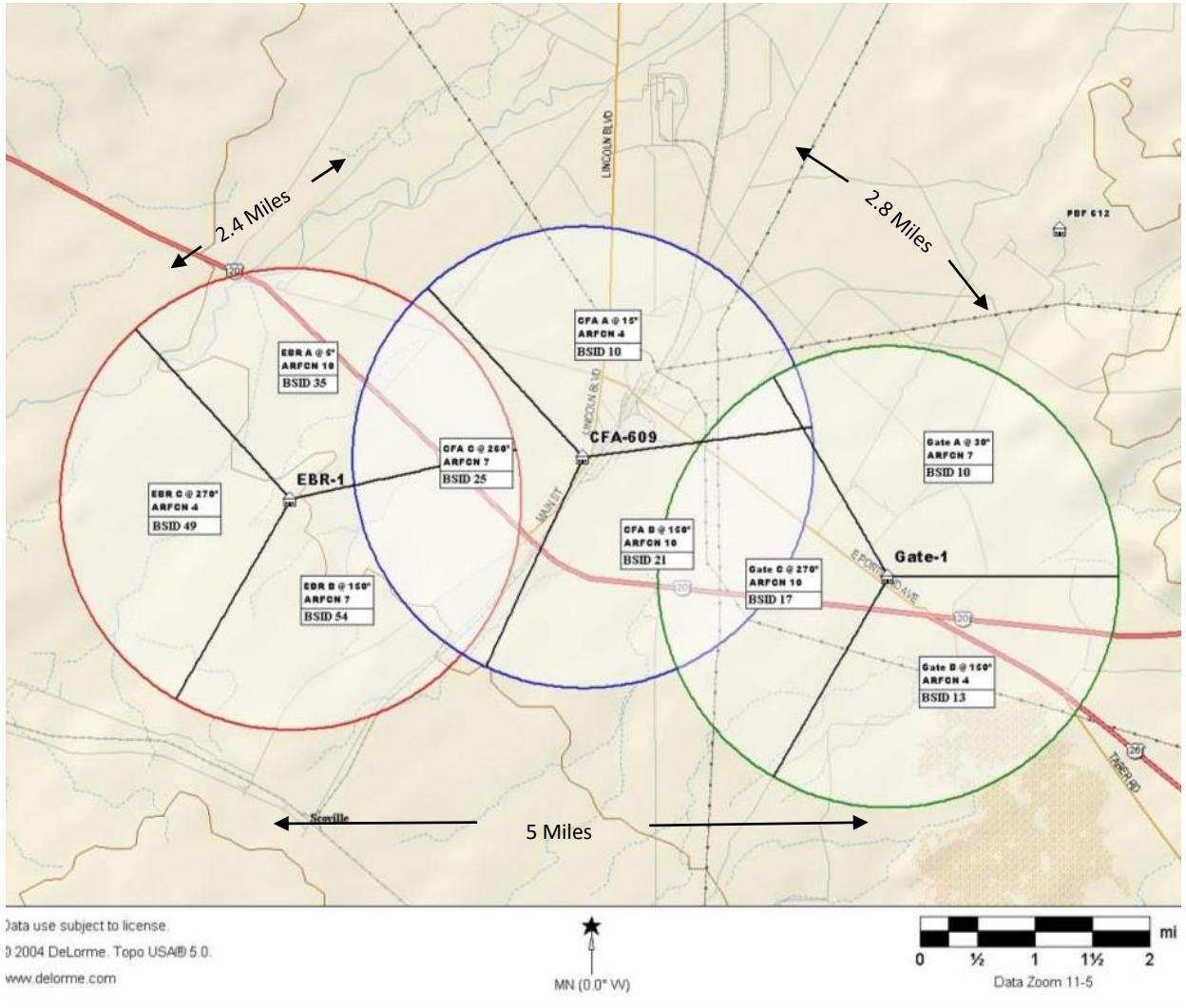
Uniquely configured for 5G use case evaluation

INL's 890 Square Miles Provides Diverse Opportunities

- **Isolated test range**
  - ✓ No nearby military bases, international airports or urban areas
  - ✓ Natural RF shield provided by caldera landscape
- **Multiple facilities and terrains**
  - Rolling high desert with surrounding mountains
  - 5000' average elevation
  - Radio site at 8628' elevation
  - Numerous test areas
  - Broadband data access
  - Controlled access
  - Secure, IP protected multi-user facility



WTB Cellular Configurations



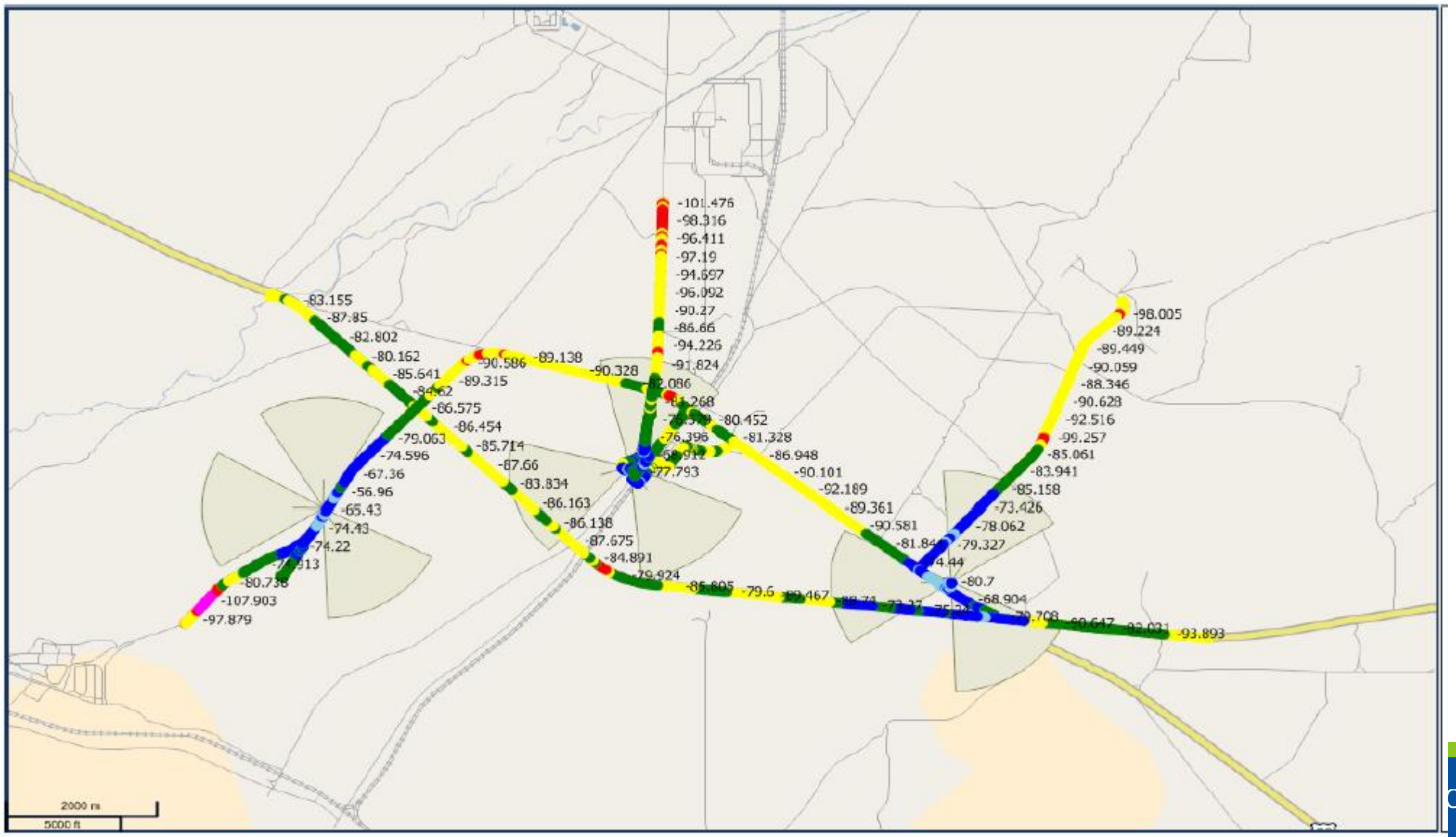
Flexible & Reconfigurable

Cellular Core:
- Handovers
- Alarms

RAN:
- Frequencies
- Power
- Antenna downtilt

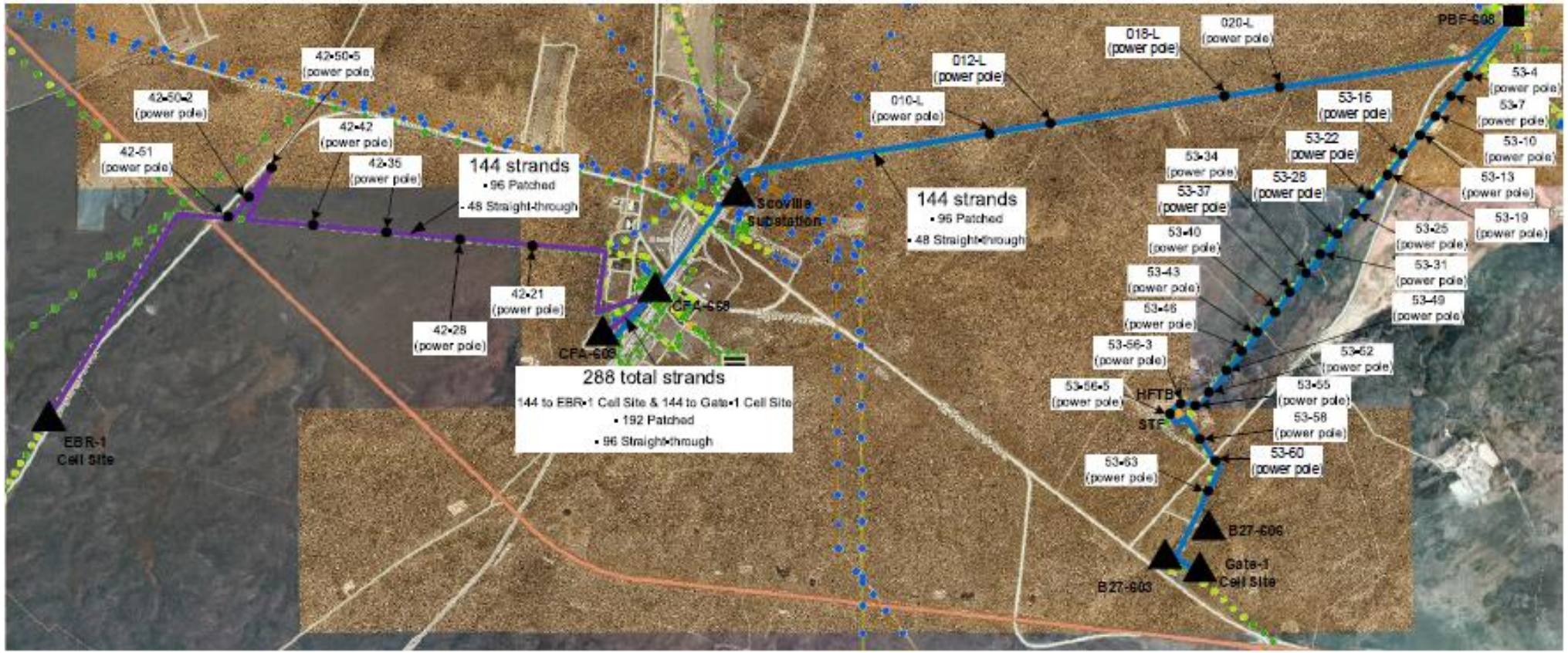
Ability to rapidly reconfigure the wireless environment and network settings to meet target area requirements

RF Optimization (RSRP)



RF Optimization (DL Throughput)

Fiber Network for Backhaul



CFA-609 – EBR-1 cell site link

CFA-609 – Gate-1 cell site link

Outdoor Pedestal Termination

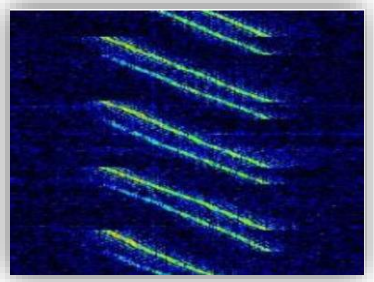
Indoor Termination

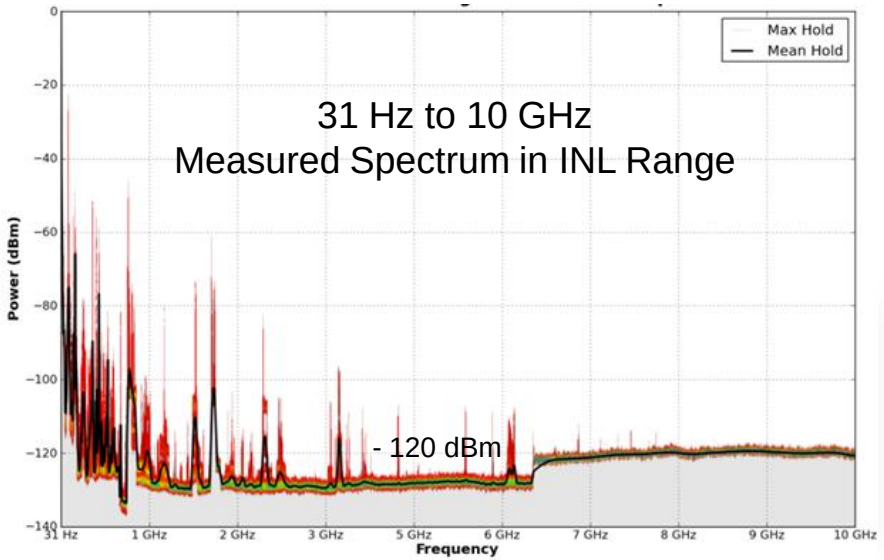
Power Pole Breakout

Spectrum Flexibility

- **NTIA Experimental Radio Station**
  - ✓ "Full" spectrum use (as outlined in NTIA Redbook)
  - ✓ Government test / experimental use only
- **Local Spectrum Manager**
  - ✓ Max Power/Frequencies case by case basis
  - ✓ Rapid approval (1 to 4 weeks) by INL Spectrum Manager
- **Real Time Spectrum Monitoring**
- **Low RF noise: typically, ≤ -120 dBm (over 10 kHz RBW)**

Monitoring Equipment





Multiple Monitoring Sites

State-of-the-Art INL WTB Assets and Capabilities

Full Scale Communications Test Networks

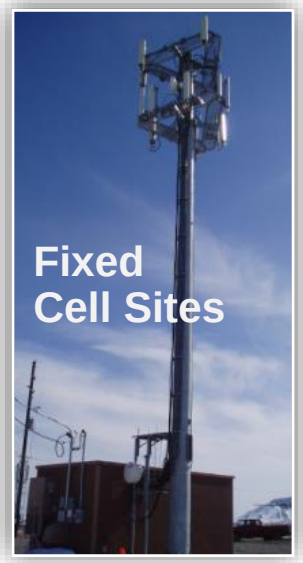
- ✓ 5G SA & 5G NSA Tier I Carrier Grade Network (in progress)
- ✓ 4G LTE, 3G UMTS & 2G GSM Tier I Carrier Grade Networks
- ✓ LMR radios and repeater systems
- ✓ HF fixed and mobile radios / antennas
- ✓ Isolated Satellite system
- ✓ Mountain top line-of-site access

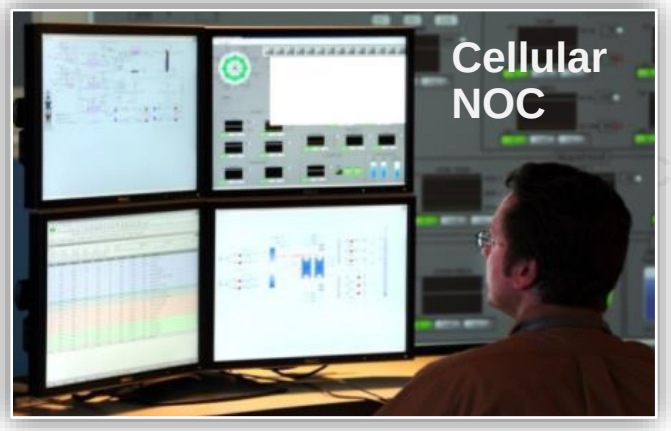
Instrumentation:

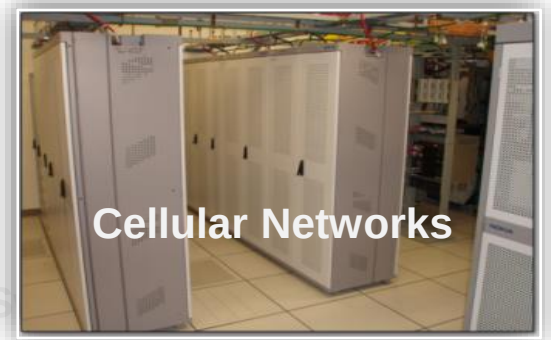
- ✓ RF waveform analyzers
- ✓ Noise generators for controlled interference
- ✓ Protocol analyzers

Established Services & Processes:

- ✓ Real Time Spectrum Monitoring
- ✓ Broadband data access – entire INL Range
- ✓ Visitor – US citizen & foreign national

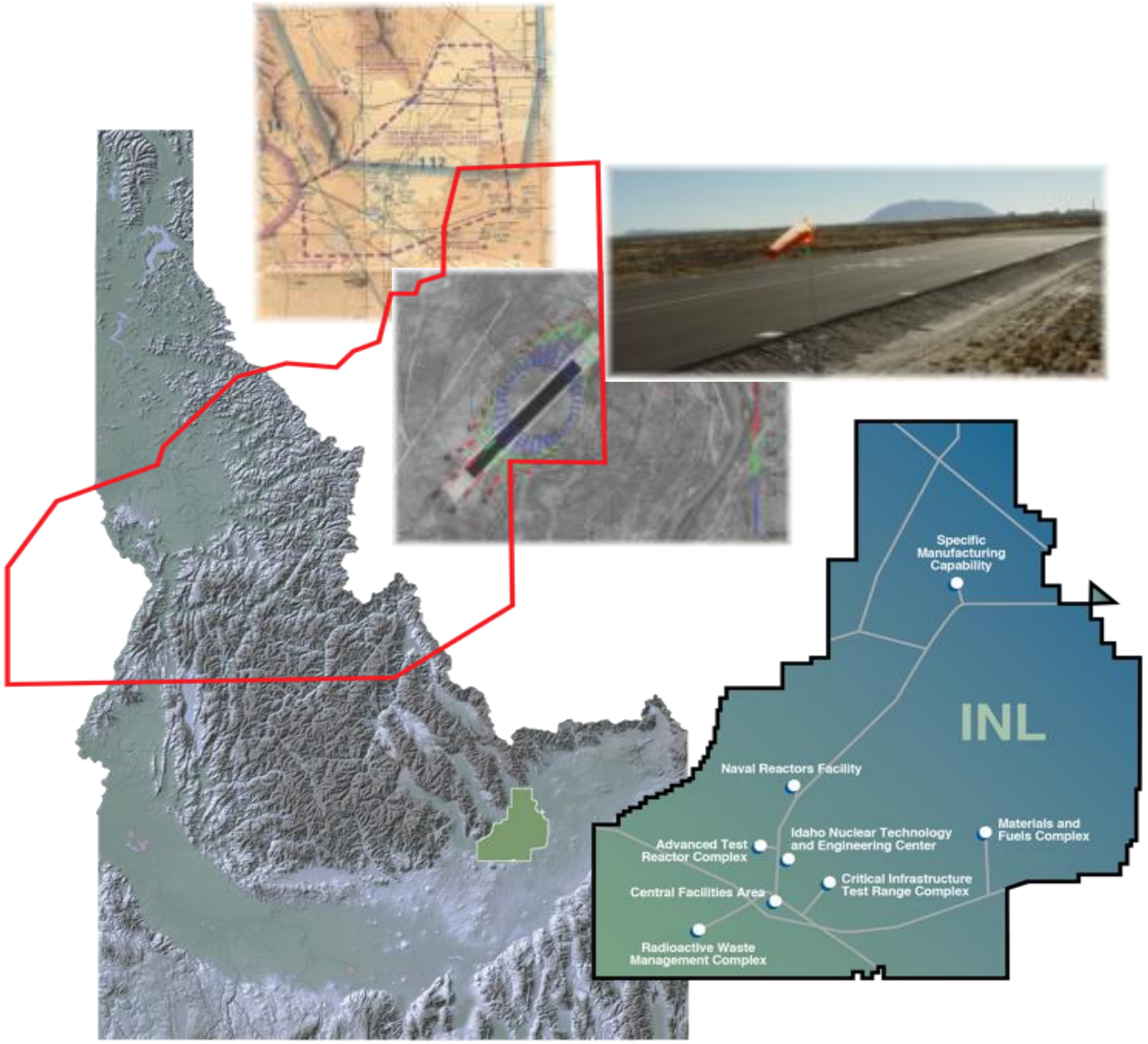






Comprehensive End-to-End Network & Engineering, Operations, Deployment & Testing Expertise

UVS Research Park



- Air space utilization through FAA 'Certificate of Authorization or Waiver (COA)'
  - ✓ Blanket COA for UAS sub-55 lb.
  - ✓ Ceiling of 9,500' MSL and ~3,100 sq miles
- Isolated controlled access boundaries for testing
- Airfield (1000' X 100' asphalt)
- Infrastructure and support facilities
- DOE UAS Center of Excellence

Future directions

- Remote base stations
  - ✓ Hosting remotes sites
  - ✓ Providing remote sites
- Increased academic research
- Remote accessibility with needed security
- Support of multi network 5G configurations such as Multi Operator RAN (MORAN)

Idaho National Laboratory