IoTs Public Key Infrastructure using Reconfigurable Hardware Root of Trust

Sunday Ekpo, Liangxiu Han, Muazzam Zafar, Sunday Enahoro, MfonObong Uko and Andy Gibson

Dr Sunday Cookey Ekpo, *PhD, CEng, SFHEA*

Communication and Space Systems Engineering Research Team,

Smart Infrastructure and Industry Research Centre,

Manchester Metropolitan University, UK

E: S.Ekpo@mmu.ac.uk; Twitter: scookey

Outline

- Background;
- Internet of Things (IoTs) Sensors Connectivity;
- IoTs Public Key Infrastructure;
- Reconfigurable Hardware Root of Trust Concept; and
- Conclusion and Collaboration Opportunities.

Background & Current Industry-linked R&D

- RF, Microwave and Millimetre-wave Devices:
  - GaAs pHEMT Low-Noise Amplifiers;
  - GaN/SiC HEMT Power Amplifiers;
  - Reconfigurable/Tunable Switches;
  - Hybrid Power Dividers and Combiners;
  - Reconfigurable Power Dividers.

- MIMO, SISO, MISO & SIMO Antennas for 5G;
- Satellite Broadcast Solutions Manufacturing;
- RF Antenna Biosensors Development;
- Industrial IoTs Sensors Characterisation;
- Fibre-Integrated Reception System;
- Circuit-emulating Embedded Systems Design.

Wireline & Wireless Comms;
Industry 4.0 & Smart Manufacturing;
Water Resources;
Energy.

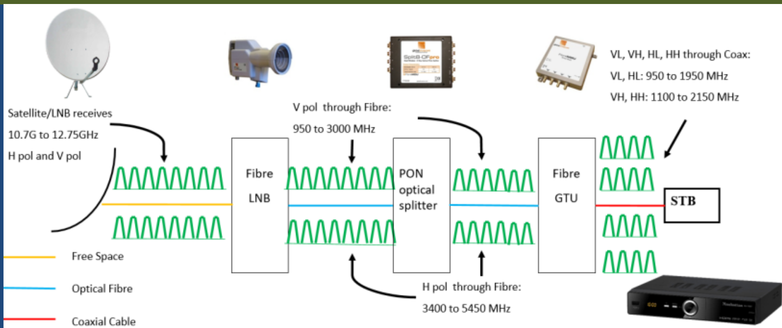
Healthcare;
Transportation;
Sustainable Infrastructure;
Environmental Monitoring.

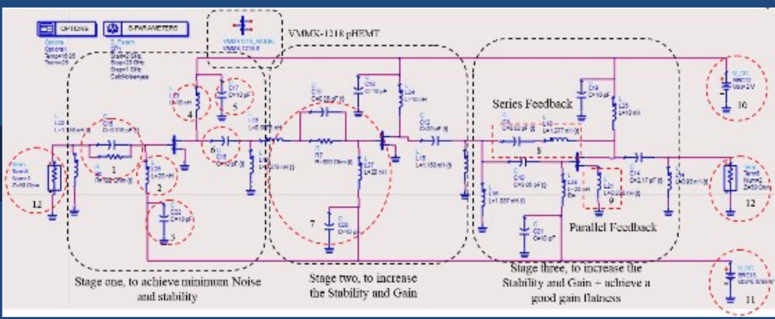
New Research Interests

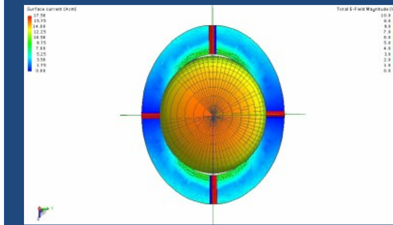
- **RF/Microwave Biosensor Development for Point-of-Care Diagnosis;**
- **Artificial Intelligence Applications in Radio Communication Systems & Industry 4.0;**
- **Reconfigurable RF Antenna, Isolators, Circulators and Switches;**
- **AI-enabled Smart RF Exposure Measurements and Calibration;**
- **Smart Satellite-Cellular Internet of Things Convergence Connectivity Ecosystem.**

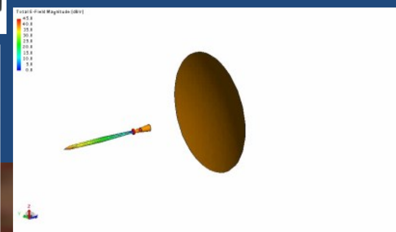
Manchester Met is a world-leading University for future-generation adaptive high frequency components and space systems engineering design, modelling, simulation and development.

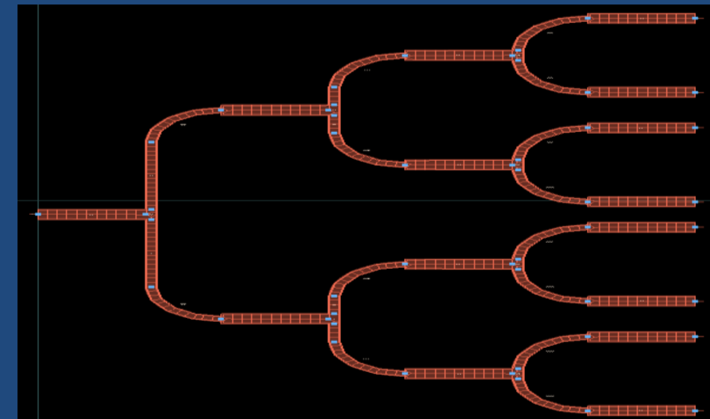
RF, Microwave & Millimetre-wave R&D Projects

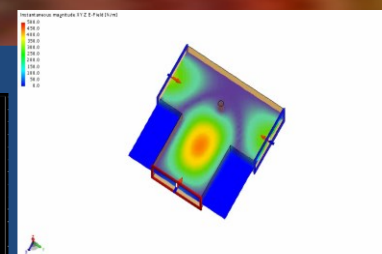


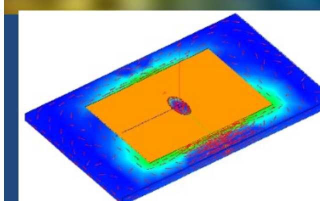


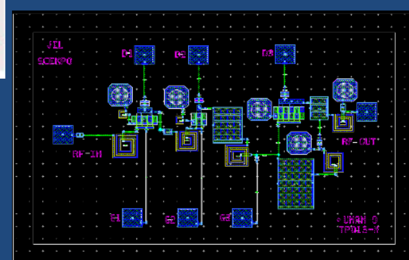


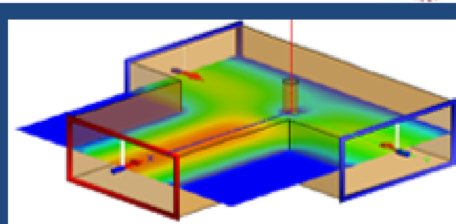


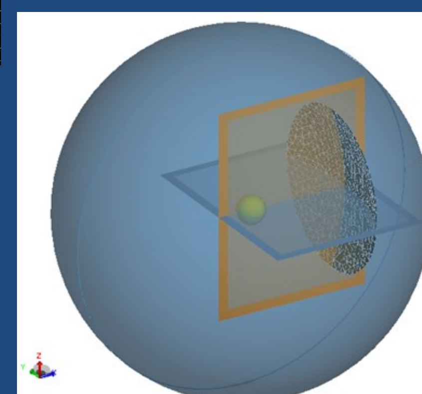


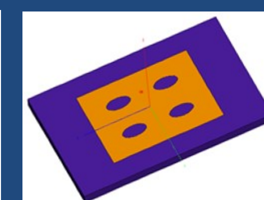


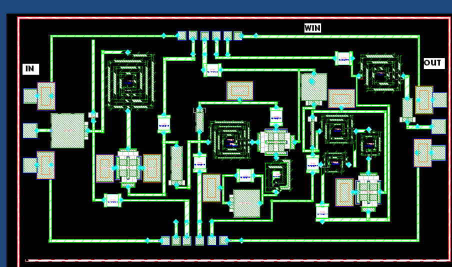


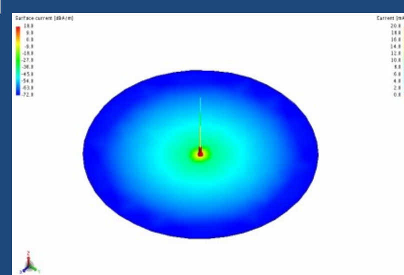


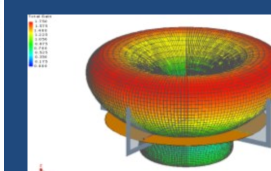


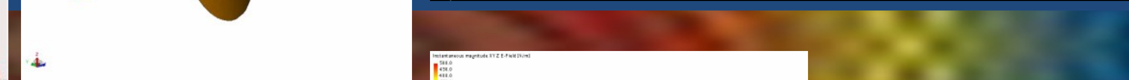




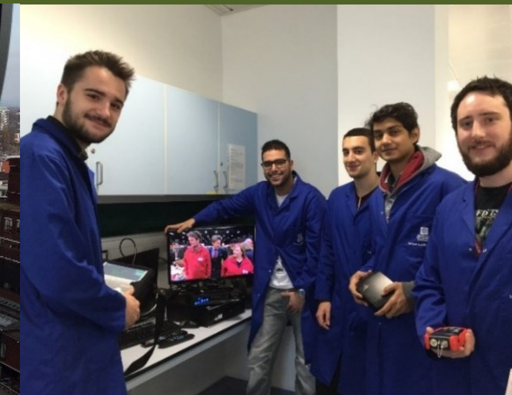






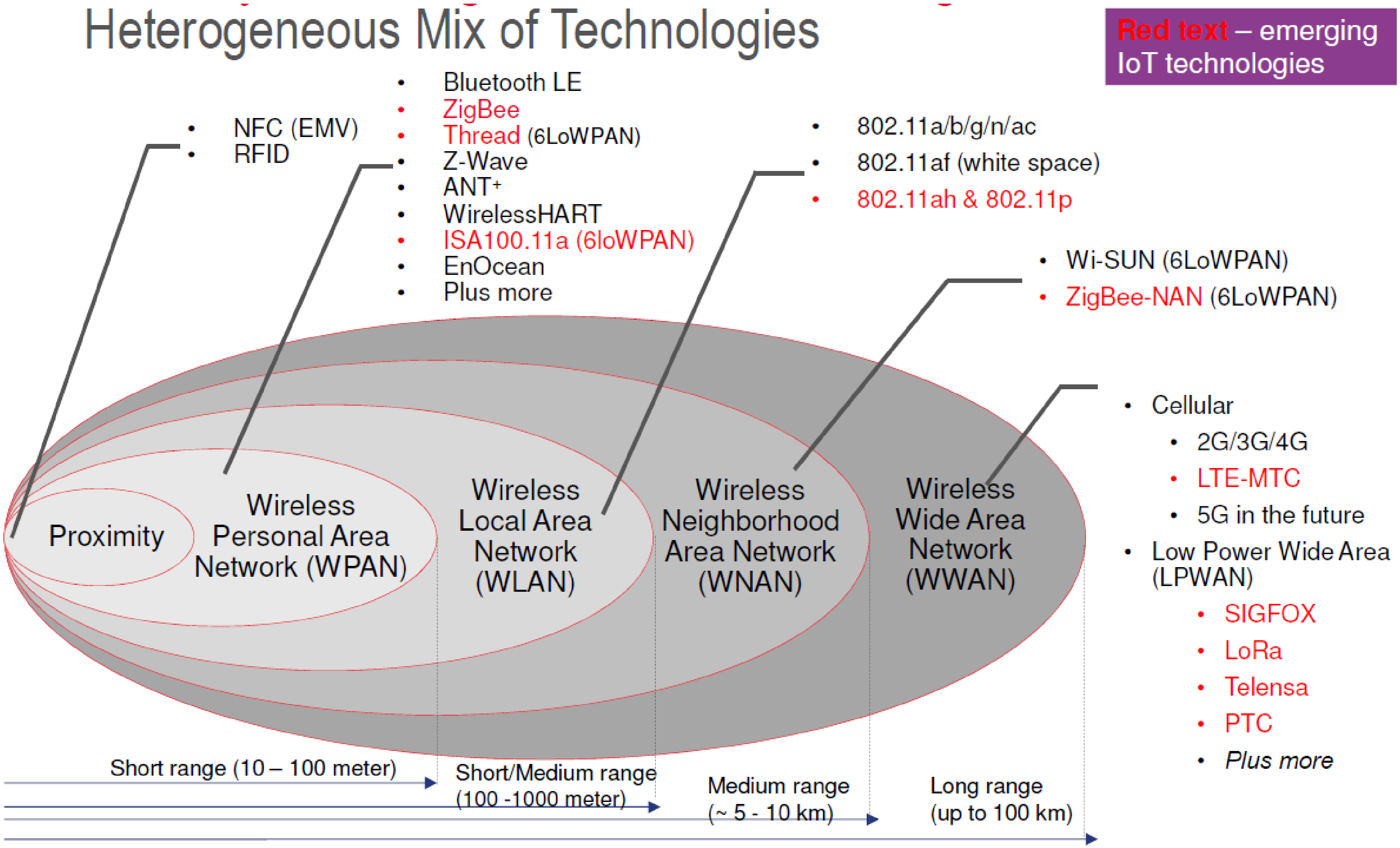


Communication & Space Systems Engineering Team



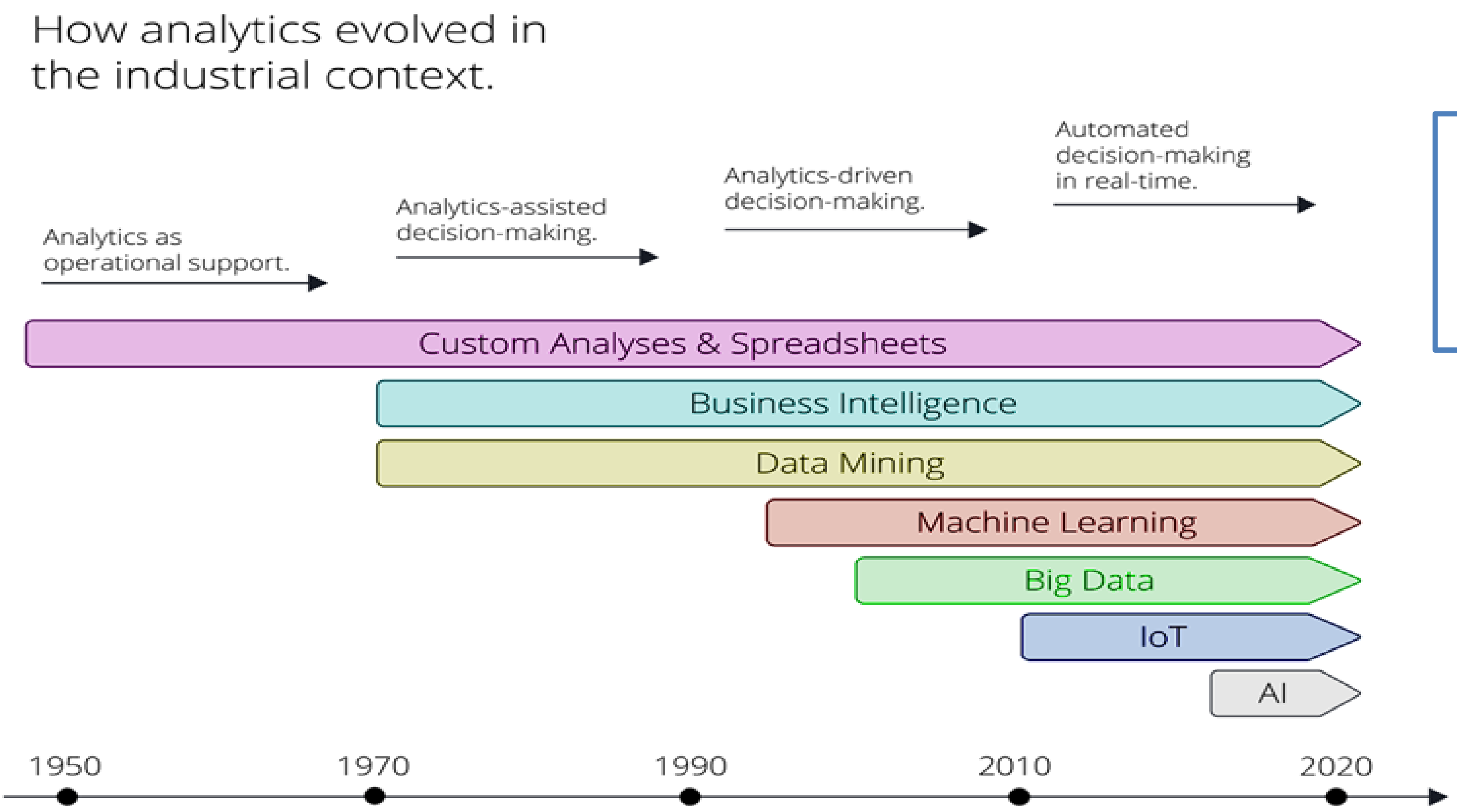
Internet of Things Sensors Connectivity

- Enabling Wireless Technologies for IoTs: 5G WWAN



Source: Keysight Technologies UK Ltd, Keysight Solutions for IoTs and M2M, 2015.

Industrial Analytics Evolution



IIoTs optimise efficiency, increase overall equipment effectiveness and minimise costs.

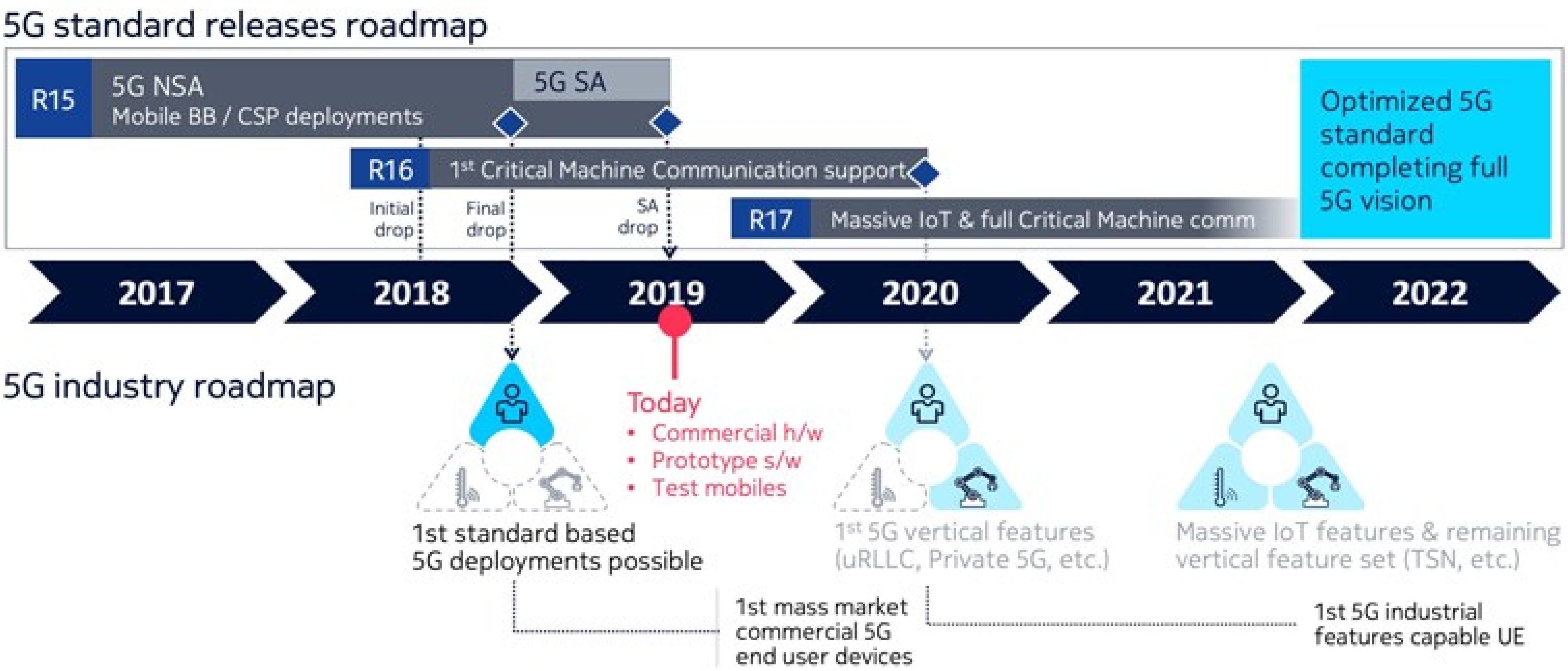
IIoTs Evolution – enables transition from data-assisted decision-making to automated decision-making in real-time.

Source: WIN Semiconductors Corporation (2016).

5G-enabled IoTs & Open RAN Ecosystem

Industrial Internet of Things:

- **Third Phase of the Internet versus Fourth Industrial Revolutions**

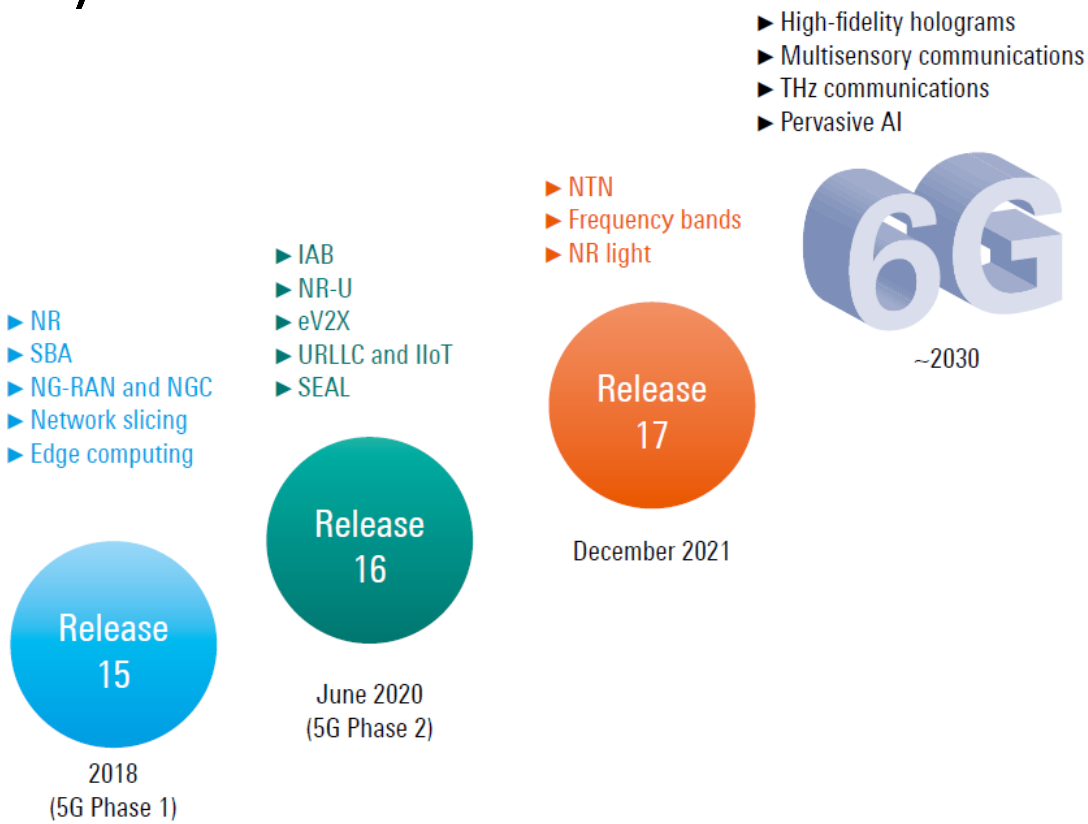


Source: WIN Semiconductors Corporation (2016).

Auxiliary Computing Technologies for 5G/5G+ IoTs

- Auxiliary Computing Technologies for 5G/5G+ IoTs:
  - Distributed Computing (DC);
  - Edge Computing (EC);
  - Parallel Computing (PC).

Evolution Path from 5G to 6G

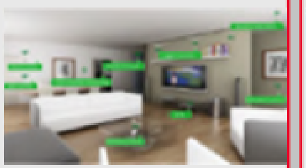


IoTs Use Cases and Applications

Internet of Things: Third Phase of the Internet Revolution

- No single wireless technology can provide the connectivity for all IoTs use cases.

Smart Home



- Security & alarm
- Light control
- HVAC control
- Remote control
- Door control
- Energy efficiency
- Entertainment
- Appliances

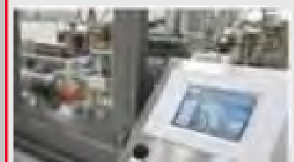
Wearables

- Health monitor
- Fitness trackers
- Smart watch
- Smart glasses
- Smart bands
- E-textiles
- Hearing-aid

Smart City

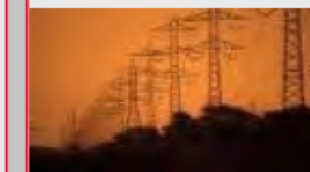
- Traffic management
- Water distribution
- Waste management
- Security
- Lighting
- Environmental monitoring
- Infrastructure
- Parking sensor

Industry Automation



- Smart machine
- Surveillance camera
- Factory automation
- Asset tracking
- Logistics and optimization of supply chain

Smart Energy



- Generation & trading
- Transmission
- Distribution & metering
- Storage
- Services

Connected Car

- V2V / V2X /V2I communications
- eCall
- Infotainment
- Traffic control
- Navigation
- Autonomous vehicles
- Maintenance

Wireless Connectivity

Source: Keysight Technologies UK Ltd, Keysight Solutions for IoTs and M2M, 2015.

IoTs Public Key Infrastructure

- The public key infrastructure (PKI) is currently the industry's holy grail for building secure IoTs devices.

- The current PKI design solutions lack:

(i) post-manufacturing multi-radio dynamic key reconfiguration;

(ii) integrated reconfigurable hardware solutions.

- PKI must be embedded into the hardware design and simplified for third-party developers and manufacturers to implement and deploy.

IoTs PKI Use Cases

- Real-time Non-Terrestrial-Terrestrial Connectivity;
- Trusted Identity and Provisioning;
- On-Device Key Generation;
- Offline / Limited Connectivity;
- Secure Boot and Code Signing;
- Mutual Authentication;
- Certificate Lifecycle Automation.

Source: Keyfactor (2022)

Key Considerations for IoTs PKI

- Determine where the root of trust (RoT) is hosted (internal PKI, public Certification Authority (CA) or managed PKI);
- Decide private key storage location onboard the device;
- Provisioning and commissioning process – where certificates are securely signed;
- Third-party industry requirements for an entity’s certificate validity, key size, algorithm and identity.

Source: Keyfactor (2022)

IoTs Public Key Infrastructure Cryptosystem

IoTs PKI: A Two-Key Asymmetric Cryptosystem; PKI enables different information technology nodes to have:

High-level Information Confidentiality	Strong Data Encryption	High-level Confidence

IoTs PKI Nodes

Edge	Gateway	Enterprise

Authentication Layer (Certification Authority (CA): Private or Public)

Digital Signatures (DS)	Digital Certificates (DC)

Keys

Public	Private

PKI Components: People, Hardware, Software, Policies and Procedures.
PKI Purpose: To create, store, distribute, manage and revoke digital certificates based on a two-way asymmetric cryptography.

Reconfigurable Hardware Root of Trust Concept

<table>
<tr><td colspan="6">Satellite-Cellular IoTs PKI</td></tr>
<tr><td colspan="2">Supports 5G/5G+ Radio Access Technologies</td><td colspan="2">Supplements the 5G/5G+ Cellular Radio Access Network</td><td colspan="2">Complements 5G/5G+ Cellular Services</td></tr>
<tr><td colspan="6">IoTs PKI Nodes</td></tr>
<tr><td colspan="2">Edge</td><td colspan="2">Gateway</td><td colspan="2">Enterprise</td></tr>
<tr><td colspan="6">Authentication Layer [CA: Private, Public or Peer (3Ps)]</td></tr>
<tr><td colspan="3">Dynamic Key Configuration Protocol (DKCP) [DS]</td><td colspan="3">Reconfigurable Hardware Root of Trust (RHRoT) [DC]</td></tr>
<tr><td colspan="6">Authentication Layer Tiers</td></tr>
<tr><td colspan="2">DKCP [Strong]</td><td colspan="2">RHRoT [Stronger]</td><td colspan="2">DKCP & RHRoT [Strongest]</td></tr>
<tr><td colspan="6">Keys</td></tr>
<tr><td colspan="3">Public</td><td colspan="3">Private</td></tr>
</table>

Conclusion: Sat-Cell IoTs PKI Security Metrics

- The strength of an encryption is proportional to the cryptographic keys and algorithms that support it.

- Table 1 shows the smart satellite-cellular IoTs PKI security logic metrics.

Table 1. Smart IoTs PKI Security Logic Metrics

IoTs PKI	**IoTs PKI**	**Security Logic Metric**	
RHRoT	**DKCP**	**Output**	**Level**
0	0	0	Weak [OR / AND]
0	1	1	Strong [OR]
1	0	1	Stronger [OR]
1	1	1	Strongest [AND]

Conclusion: Key Message

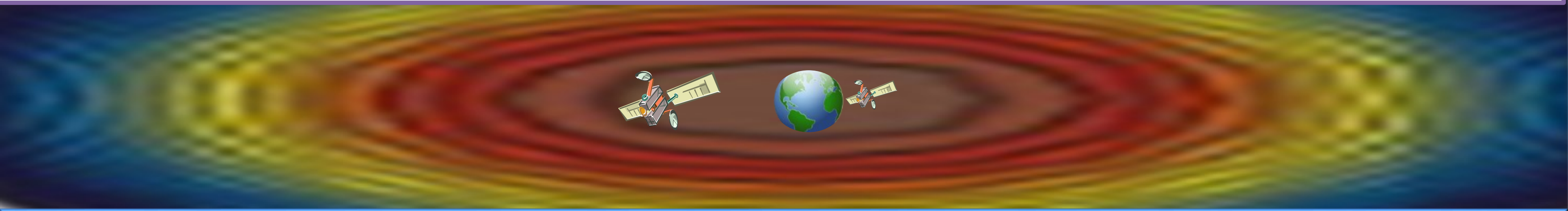
- The proposed hybrid hardware-application protocol security solution provides a three-tier authentication that can be optionally implemented depending on the threat level within the IoTs device environment.
- This solution can be implemented to achieve IoTs PKI-based authentication, encryption and integrity for devices at scale by device manufacturers with little or no cryptography knowledge.
- The proposed adaptive IoTs PKI model promises scalable ubiquitous, seamless, cost-effective, secure, simple and security solution to stay ahead of existing and emerging threats and regulations.

Potential Collaboration Areas

- ***Reconfigurable Smart IoTs Public Key Infrastructure, Security and Cryptographic Algorithms***;
- ***Artificial intelligence*** applications in **Satellite-Cellular IoTs**;
- ***5G/6G physical layer*** radio communication components *development*;
- ***Smart Factory RF Exposure Measurement and Calibration*** for *factory entities* and *smart manufacturing* services.

Thank You.

"Manchester Met is a world leader in future-generation adaptive high frequency components and space systems engineering design, modelling, simulation, characterisation and development."



Any Questions Please?

E: S.Ekpo@mmu.ac.uk; Twitter: scookey