UNIVERSITY of STRATHCLYDE
PNDC

PNDC Workshop in Communications and Cyber Security for Smart Grids

1st of Dec 2022

Opening and welcoming

- PNDC workshop is part of the IEEE International Conference on Smart Applications, Communications and Networking (SmartNets 2022)
- It is an industry-centred event featuring the latest communications and cyber security challenges and promises in smart grid applications.
- It brings together industrial partners, technology providers, policy makers, and academics to share ideas and talk about various important aspects such as, synchronisation, challenges of spectrum access, cyber security and current 5G interests in Grid Digitalisation.

- **Dr Jacqueline Redmond**
- **PNDC Executive Director**

EVOLUTION

Cyber Security 2023

Agenda

Welcome & Opening, Jacqueline Redmond/ Federico Coffele/Kinan Ghanem,

Comms & *security challenges in smart grid: the importance of validation, James* Irvine,

Global challenges of spectrum access for smart grid applications, Adrian Grilli

Digitalisation of Energy with 5G Secure Communications for low carbon grid transformation, Nigel Nawacki,

Sync and Timing for secure Critical Infrastructure, Chris Farrow

Debswana Smart Grid Solution, Karabo Mmokwa

Zero Trust security in OT, Chris McGookin,

Agenda

Welcome & Opening, Jacqueline Redmond/ Federico Coffele/Kinan Ghanem,

***Comms & security challenges in smart grid: the importance of validation*, James Irvine,**

Global chall *cess for smart grid applications*, Adrian Grilli

Digitalisation *ligel* Nawacki,

Sync and Tim *l Infrastructure*, Chris Farrow

Debswana S *rabo Mmokwa*

James has more than 25 years' experience working in research and standardisation work in mobile radio and security from 2.5G to 5G.

The academic lead for the communications: systems, integration and security theme at the PNDC.

PNDC
UNIVERSITY of STRATHCLYDE

Communications and security challenges in smart grid:

The importance of validation

James Irvine
University of Strathclyde

The big picture…

PNDC
UNIVERSITY of STRATHCLYDE

Increasing demands on the grid

- Electrification of heat, transport, etc – x3 demand in the UK for example

Low carbon generation

- Small, distributed power sources

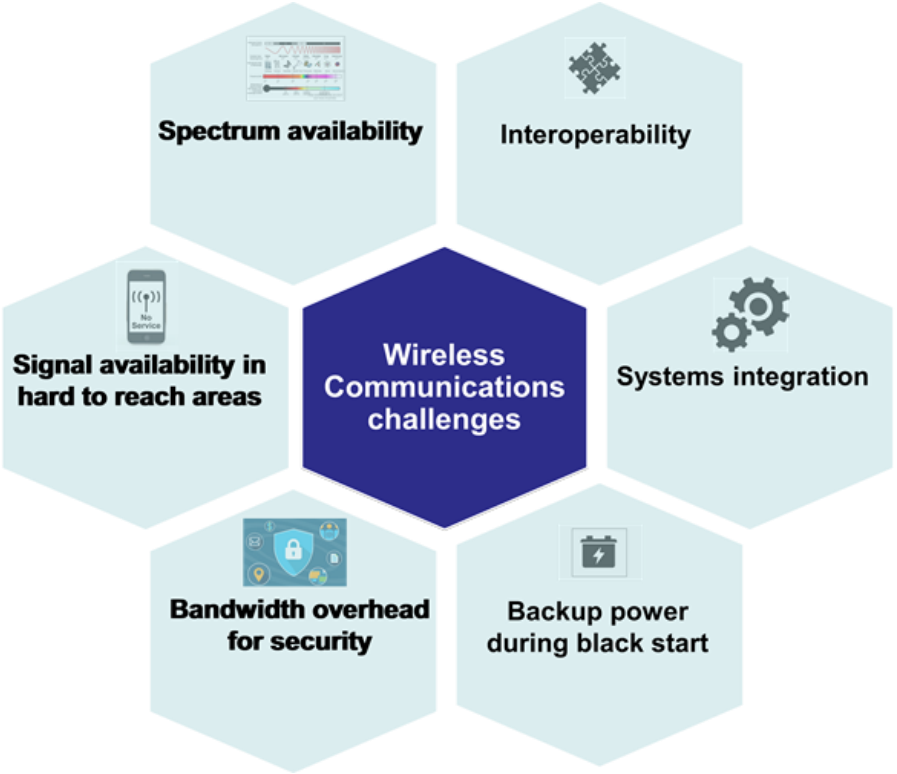
More flexibility and better efficiencies through control

- Lay fibre not copper

More challenges for the communications network

- Comms failures now lead to power failures

Some of the Challenges…



What we need…

UNIVERSITY of STRATHCLYDE
SECURITY & RESILIENCE
RESEARCH CENTRE

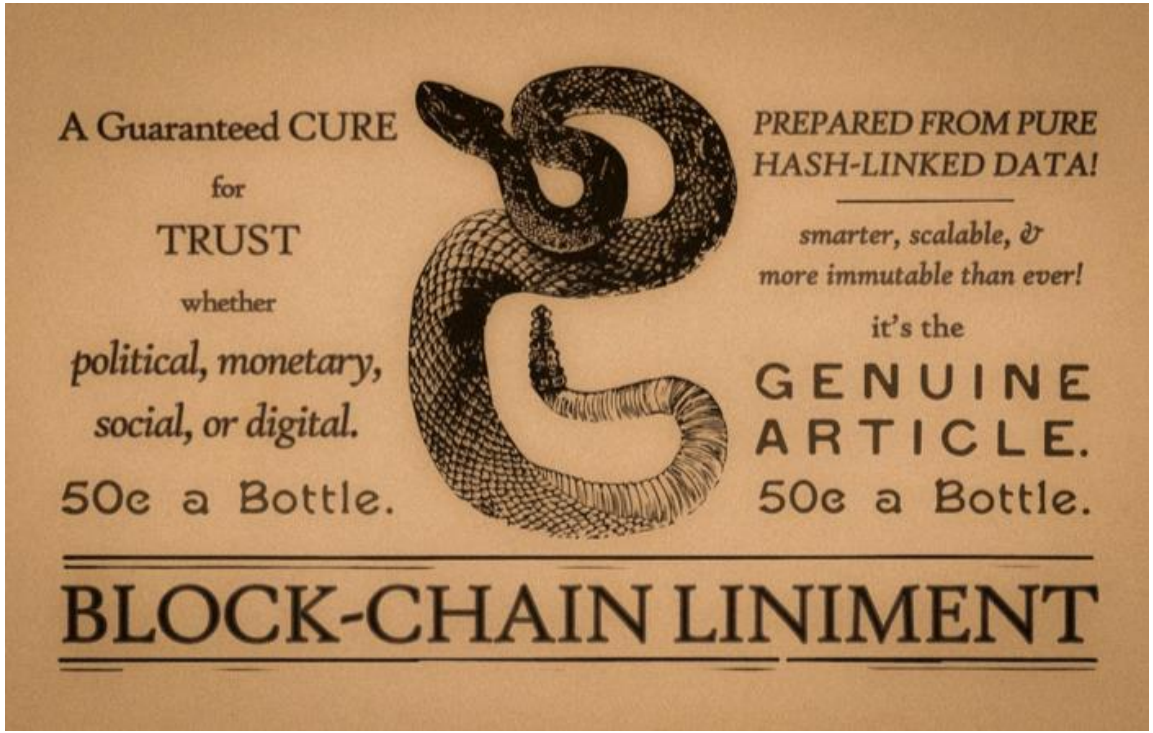
PNDC
UNIVERSITY of STRATHCLYDE

Practical, **secure** and **resilient** deployments which allow to **reduced costs**

- Best practices for **secure resilient communications**, supporting sensing, control, and self management (e.g. **virtualization**)
- A strategy for a **reliable wireless communications ecosystem** for the utilities sector, utilising **COTS** where possible

- IT and OT are converging (**colliding?**) rapidly but very different mindsets and mentalities
- Virtualisation and containerisation offer benefits but **risk reducing resilience** through improper implementation
- Security in **OT begins with the architecture** and must match what is actually being deployed
- **Legacy insecure protocols** which need to be integrate with secure networks & **3rd parties**
- **Supply chain attacks** (Solarwinds, MS Exchange, Kaseya)
- Availability > {Confidentiality, Integrity}? **Not necessarily in a distributed energy resource world**

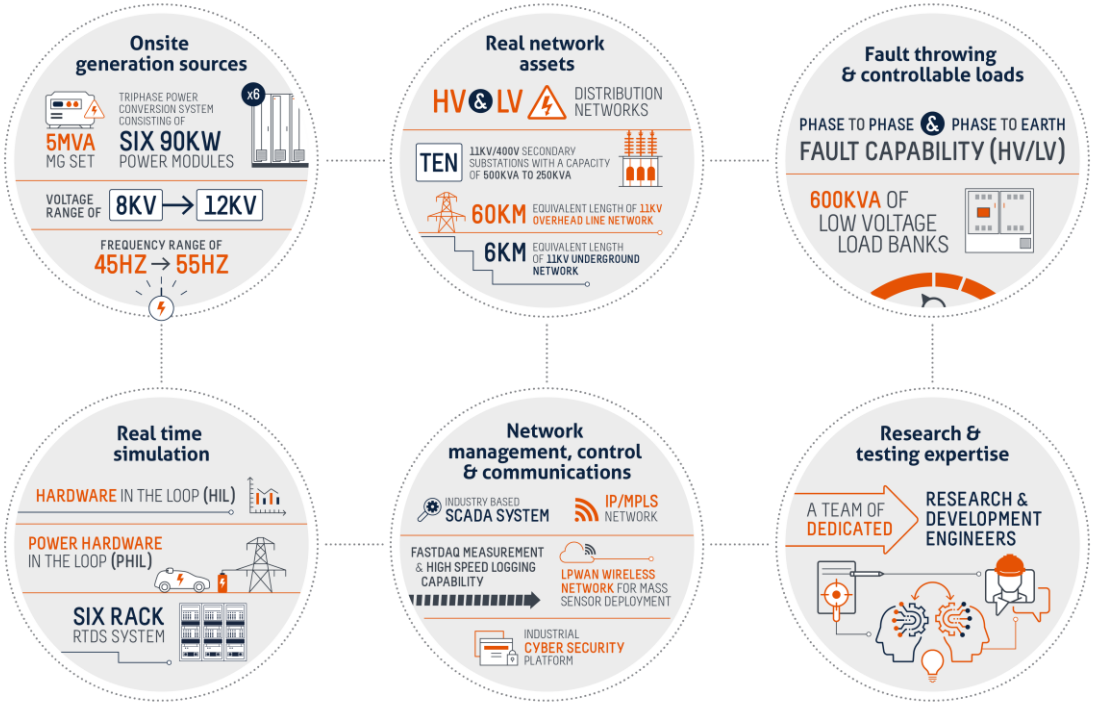
So prove it…



bitcoin.com

PNDC
UNIVERSITY of STRATHCLYDE

PNDC testing & demonstration capability



- IP/MPLS network, optical core, redundant copper rings
- WiFi and LPWAN wireless networks
- Two 5G networks being deployed
- Two SCADA networks based on industry standard configuration (from member DNOs' deployed equipment)
- Separate airgapped network for intrusion/penetration testing
- ICS equipment (RTUs and IEDs)
- Connection to wide area simulation for large scale testing
- PNDC model allows member and PNDC staff to work hand in hand on security projects; Knowledge Exchange Forums

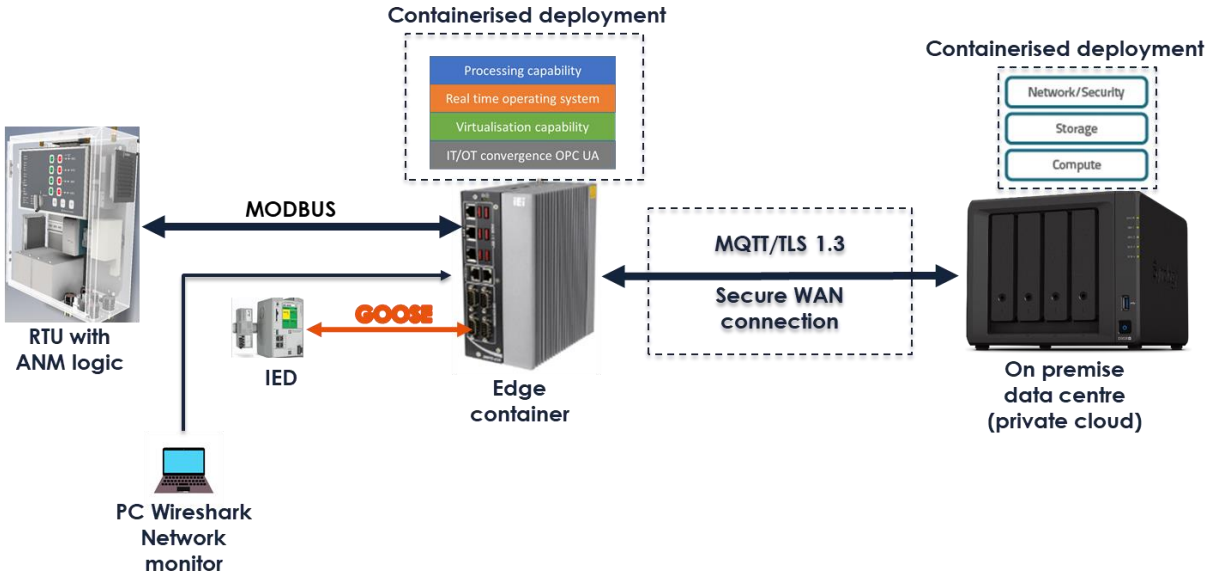
Some Practical Examples

Proving real world benefits

- Secure virtualization in a CNI environment
  - What are the benefits?
  - How can we deliver securely?
  - Practical experience
- Resilient 5G deployment
  - What are the benefits?
  - How can we deliver reliability?
  - Practical experience

Low-Latency Edge Containers for Wide Area Control of Energy Systems

- Testbed developed with a low power/cost edge device (protocol conversion)
- Testing and documentation of migration of simple ANM functions to new platform
- Security considerations of virtualized platforms in a CNI environment



Low-Latency Edge Containers for Wide Area Control of Energy Systems

Key learnings so far…

- Development – maintenance – manage-update of software
  - Additional resources from 3rd party software developers are needed
  - DNOs need to have a good understanding of the system
- Lack of 3rd party integration/Communication with the vendor end device (IT/OT)
  - Responsibility: who will take responsibility when things go wrong ?
  - Traditional vendor or new vendor the 3rd party software developer
- Cybersecurity
  - another vector, another path to exploit the system

Virtualization Test Strategy

Developed for the Constellation project led by UKPN

- Link aggregation or failover ethernet support.
- Ability to update hypervisor and other critical root of trust systems.
- System configuration is not lost following a UEFI firmware update.
- Ability to update virtual machines and see the configuration/version deployed on each node.
- Ability to guarantee RAM allocation and availability for VMs, and prioritise non-guaranteed RAM access per-VM.
- Ability to pin and allocate dedicated CPU resources and/or affinity as required, to avoid unpredicted latency spikes.
- Suitable quality of service support available for PCI and network bandwidth to enable critical network traffic to be prioritised.
- Hypervisor supports consistent allocation/mapping of a physical network interface to a virtual interface, which is mapped to one VM, and is consistently addressable from within the VM.
- Hypervisor allows PCI devices to be allocated to a VM with sufficient specificity to prevent incorrect device mapping.
- All network traffic between VMs is inspectable and firewalled, without sole reliance on the operating system in the VM.
- Isolation of VM virtual network interfaces and underlying networks.
- Use of hardware-assisted virtualisation and segregation, rather than paravirtualization, with hardware IOMMU.
- Platforms used have System Management Mode (SMM) isolation in use with appropriate configuration.

Virtualization Test Strategy (continued…)

PNDC
UNIVERSITY of STRATHCLYDE

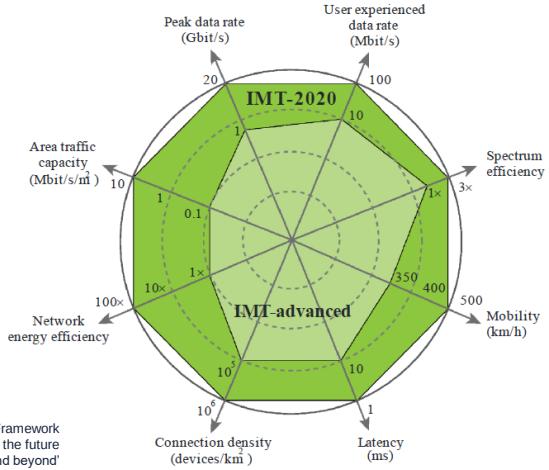
Developed for the Constellation project led by UKPN

- Platform, Hypervisor, and VM health and integrity attestation is available, robust, and meaningfully binds VM attestation to the underlying platform.
- Support for robust isolation of management services to a dedicated management plane.
- Support for multi-factor authentication on all management protocols
- Use of mutually authenticated protocols for configuration and orchestration.
- Protection of locally-held secrets through a hardware-backed root of trust.
- Potential for use of CPU-backed encrypted VMs is considered and evaluated.
- Centralised log aggregation.
- Chained system integrity validation back to the platform hardware root of trust.
- Facilitate secure hardware-backed remote attestation of integrity of hosts and guests.
- Software supply chain security and updating strategy.
- High assurance code signatures on critical code.
- Best practice, such as “zero trust” and zero touch architectures.
- Ensuring use of secure endpoint devices for privileged tasks.

5G in Practice : Latency Testing

Academic Insights activity within the Constellation Program

- 5G has ‘headline’ latencies down to ‘1ms’



ITU-R M.2083 'IMT Vision – Framework and overall objectives of the future development of IMT for 2020 and beyond'

- What can we get in practice?

- Remote shaving on the top of Snowdon…

PNDC 5G Deployments

Nokia Network

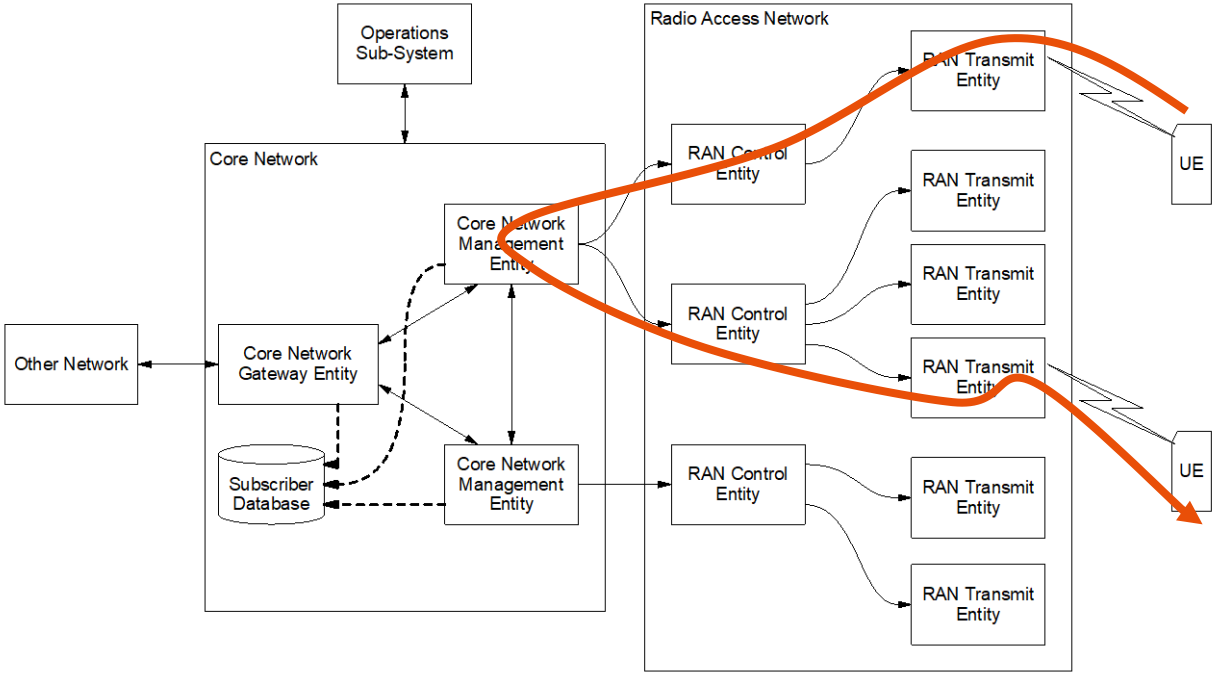
- 3.8 - 4.1 GHz 3GPP N77
- Up to 100 MHz channels
- Private network band

Ericsson Network

- 3.5 GHz 3GPP N78
- 50 MHz
- Public mobile network band

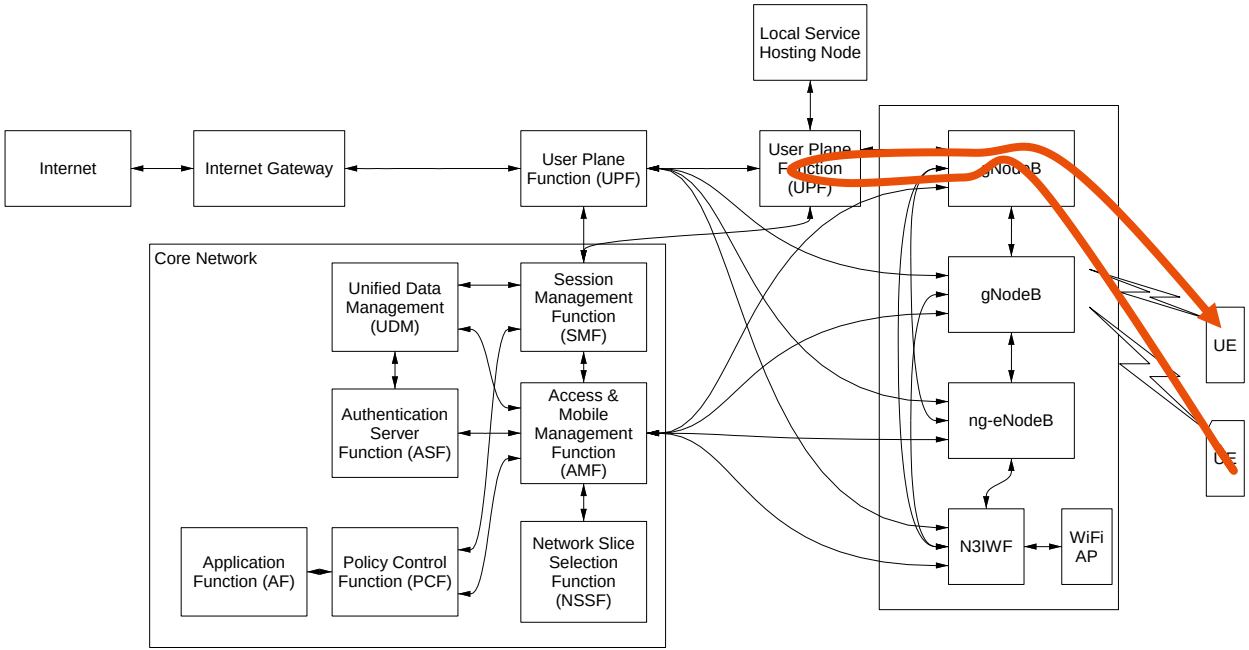
Traditional Mobile Architecture

Traffic must travel via the core



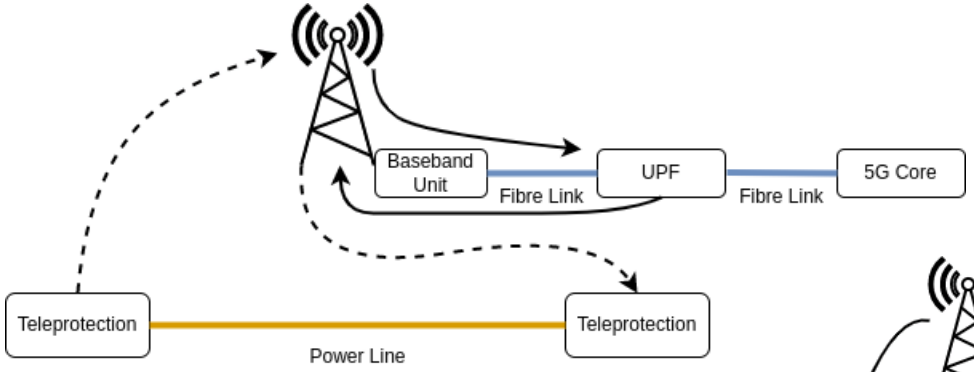
5G Mobile Architecture

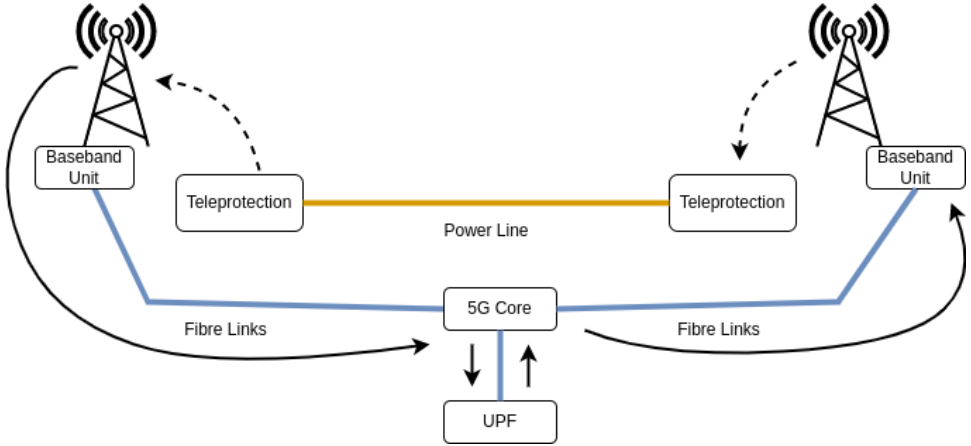
Separate control and user planes



Use Cases for Protection

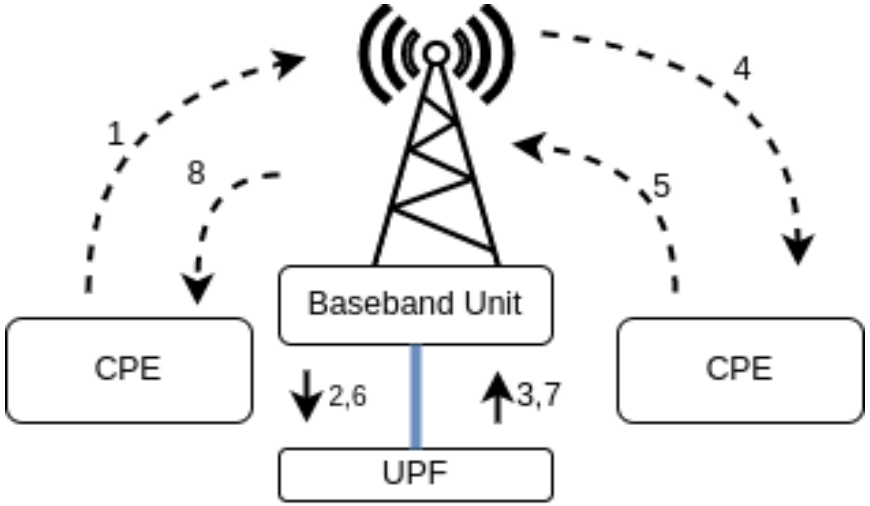
Options for single large cell, or two separate cells





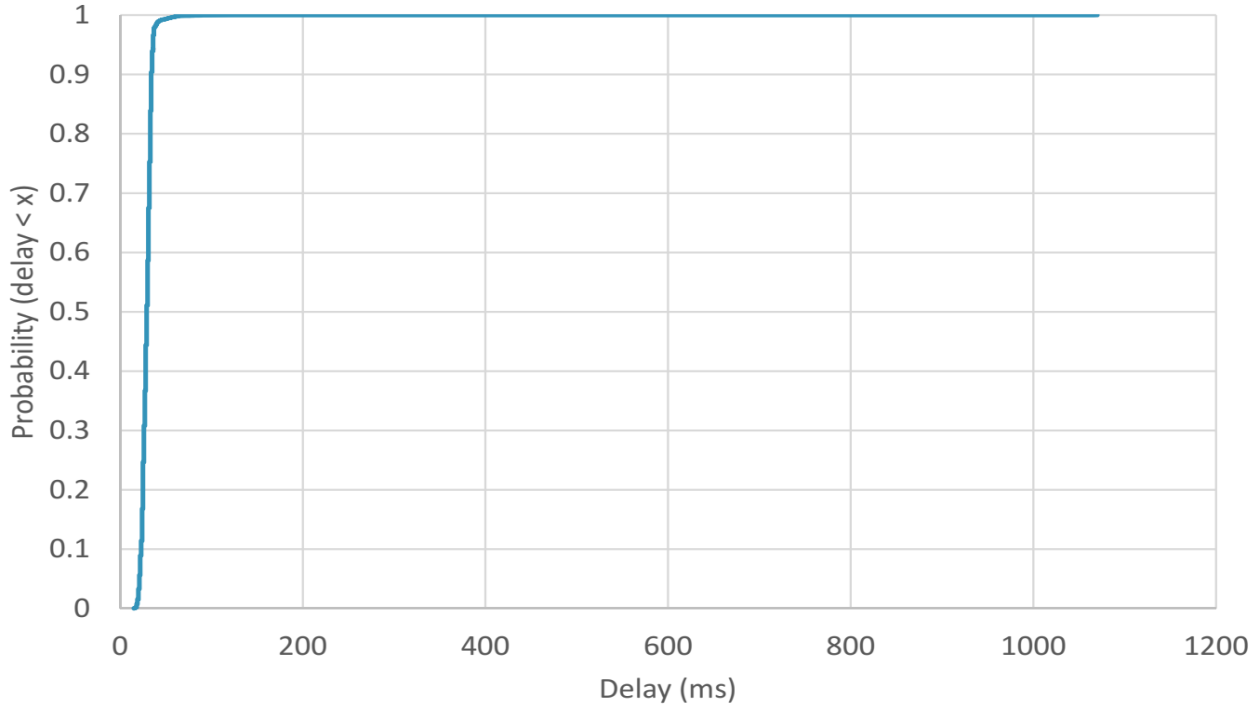
Test Scenario

End to end latency testing, local UPF, 4 radio hops



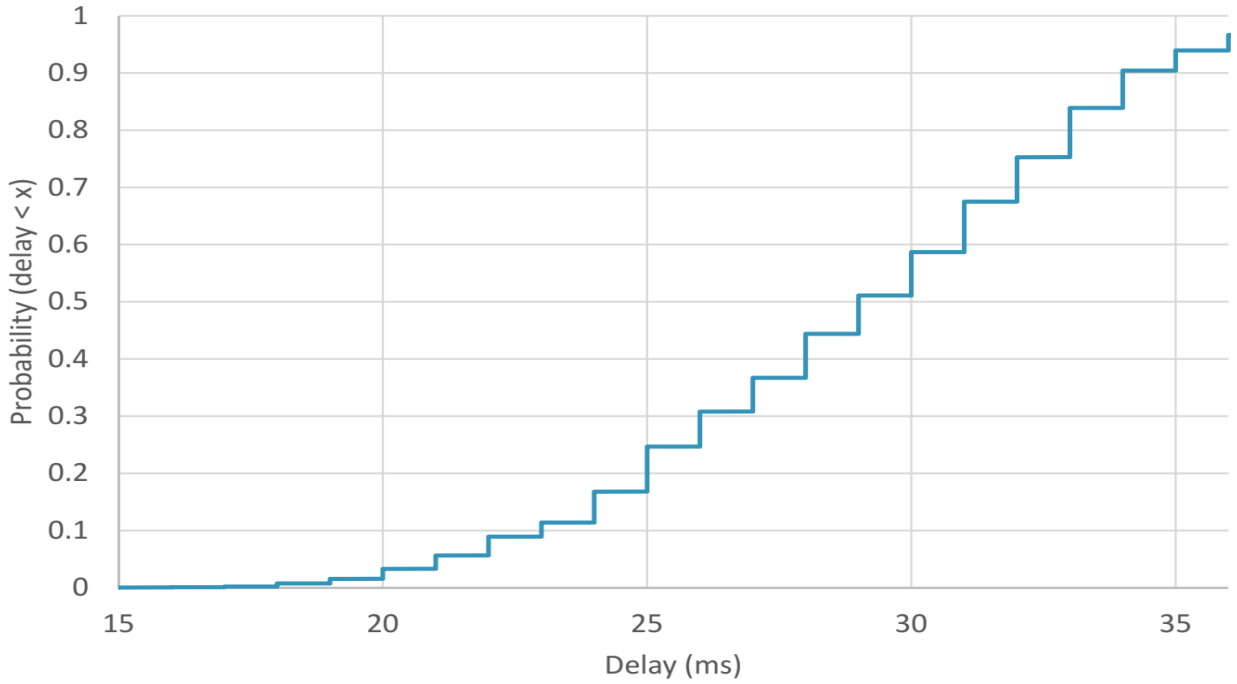
Delay Results

CDF of round trip delay (12,000 RTTs)



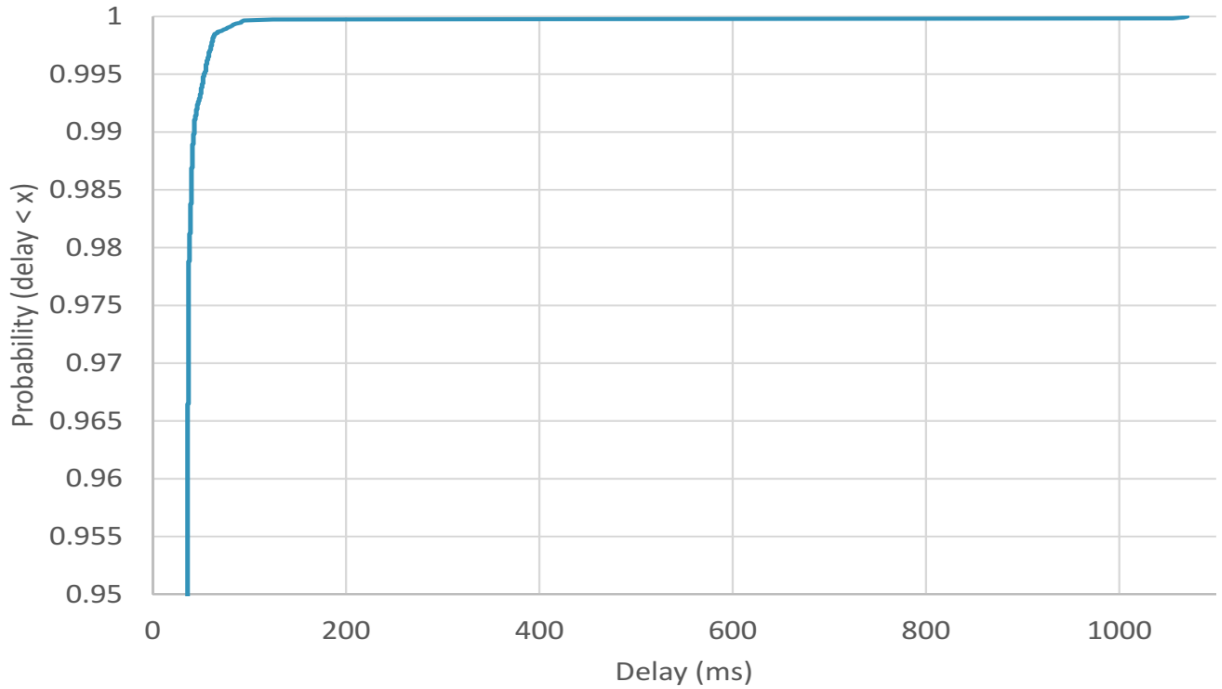
CDF of shortest 95% of RTTs

Average 29.46ms (so 15ms one way), SD 17.8ms, 99.3% of round trip times are 50ms or below



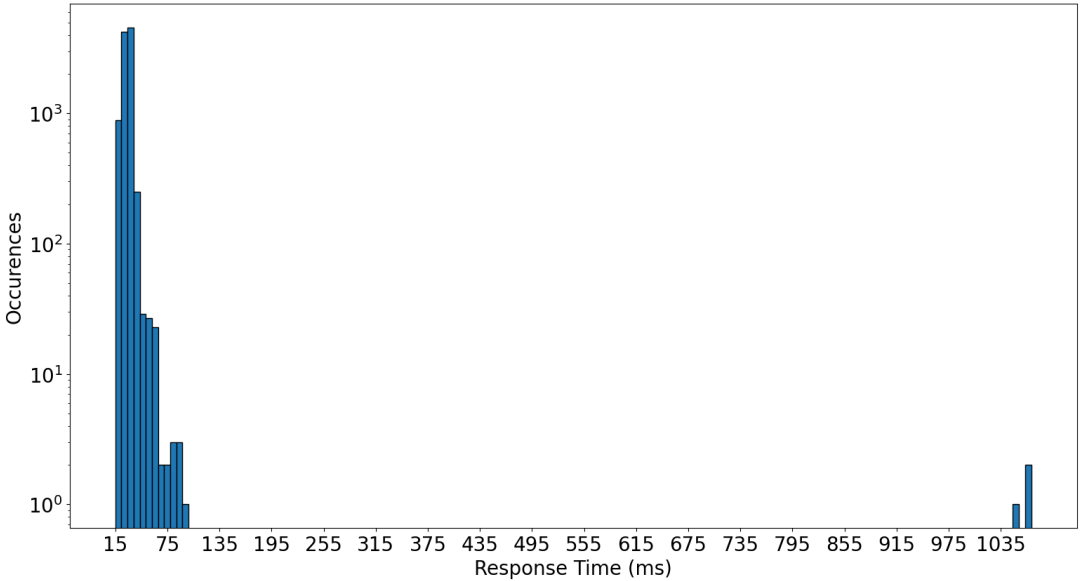
CDF of longest 5% of RTTs

99.96% of the round trip times overall are below 100ms



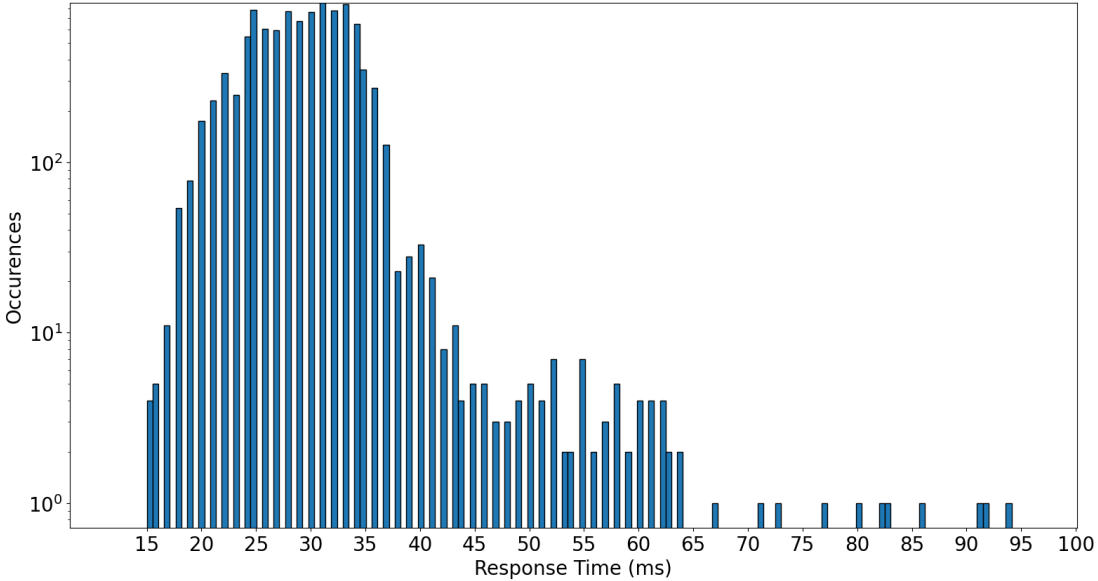
Logarithmic Display

Large gap with small number of results over 1 second



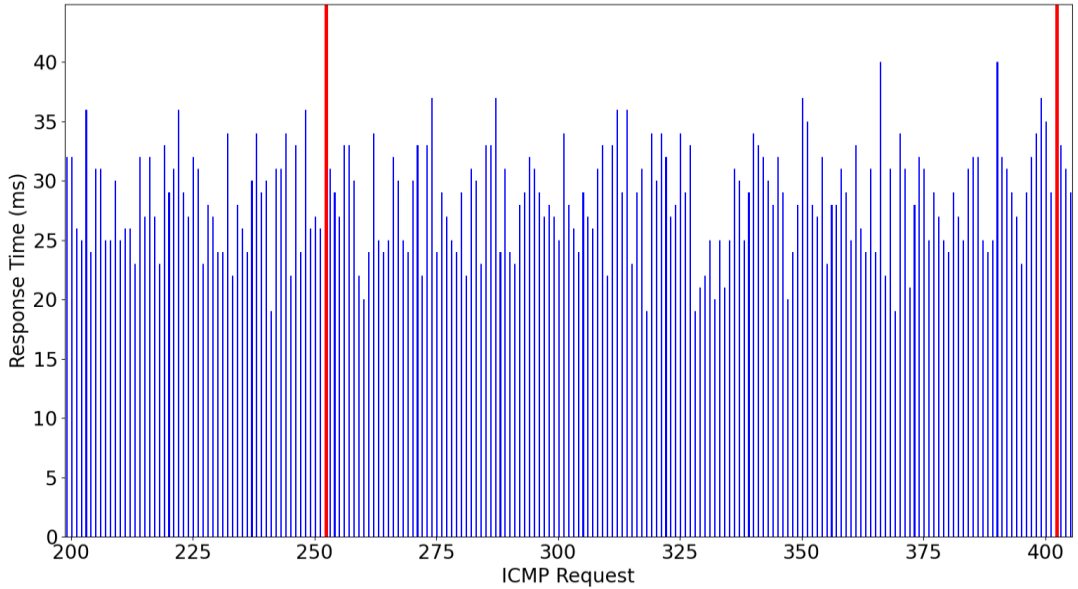
Logarithmic Display

Fairly continuous with most results below 65ms



Timeseries Display

Very long latencies occur individually and sporadically



Conclusions

More work to do!

- Discussions with other partners show a similar pattern for 4G results
- Optimisation has reduced the average times somewhat, but the outliers remain
- Possibly a missed message at the Physical Layer being resolved with a timer timing out?

- Need a better understanding of the requirements of protection – isolated issues could be mitigated by repetition
- Need to optimise average latency – 15ms is still too long
- Assumes best case – in practice there will be site to site delays

- **Shows the necessity of real world testing!**

Thank you

PNDC
UNIVERSITY of STRATHCLYDE

www.pndc.co.uk

pndc@strath.ac.uk

@pndc_uk

/company/pndc/

Agenda

Welcome & Opening, Jacqueline Redmond/ Federico Coffele/Kinan Ghanem,

Comms & security challenges in smart grid: the importance of validation, James Irvine

Global challenges of spectrum access for smart grid applications, **Adrian Grilli**

Digitalisation *ecure Communications for low carbon grid transformation*, Nigel Nawacki,

Sync and Tim *al*

Debswana S *arabo Mmakwa*

Zero Trust security in OT, Chris McGookin

Technical specialist in the UK Government in a variety of roles, including Regulation and Strategy Development, also in radio spectrum management organisation serving the electricity and gas industries in the UK

Spectrum Group Manager at the (European Utilities Telecom Council (EUTC)),

Global Challenges of Spectrum Access for Smart Grid Applications

1st December 2022

Botswana

Adrian Grilli

Technical Manager

European Utility Telecoms Council

Brussels

www.EUTC.org

EUTC

What is EUTC?

EUTC

- Represent technical and regulatory interests of Electric, Gas and Water Utilities – critical national infrastructure.
- Membership driven – with major utility from large and small utility operators including in Austria, Spain, France, Netherlands, Germany, Portugal, Ireland and UK.
- Engaging with stakeholders including vendor and operator communities to ensure alignment of new products, standards & spectrum allocation with utility requirements.
- Responding to consultations from the European Commission, Energy and Telecom Regulators and National Administrations about digitalisation of the energy sector.
- Interacting with European Parliament and Policy Groups.

Relationships with other representative bodies

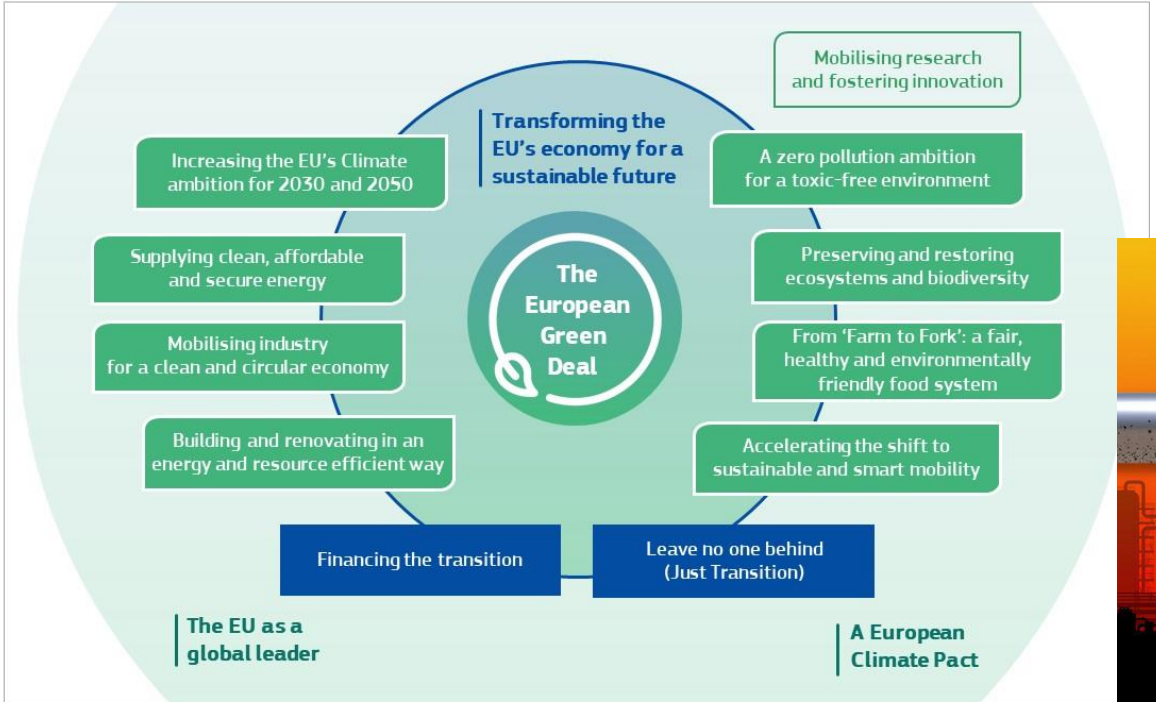
- Other UTC regions:
  - Utilities Technology Council (UTC) representing USA and Canada
  - UTC America Latina - who lead representation in ITU
  - Africa UTC - common standards with Europe in many areas
- The Critical Communications Association (TCCA); in particular:
  - the Broadband Group (CCBG) and SCADA Group
- 450 Alliance – particularly the Standards and Regulatory Group
- ETSI – System Reference Document for Utility Operations
- ITU – WP1A and WP5A on Utility Telecommunications and Smart Grids
- 3GPP (3rd Generation Partnership Project)
- CEPT, ECC, ECO, RSPG, RSG, BEREC, ITRE, EE-ISAC, ENSO, EDSO, GEODE …

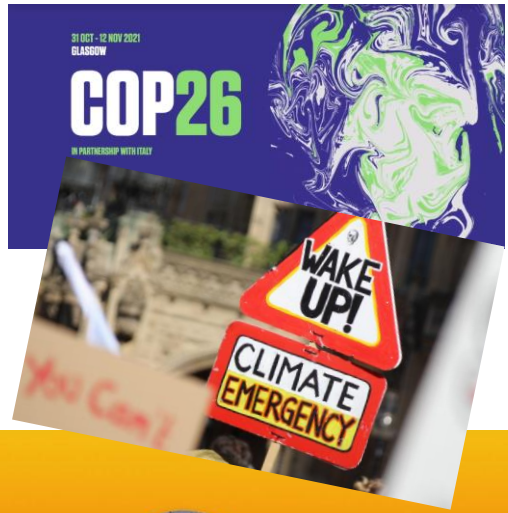
EUTC

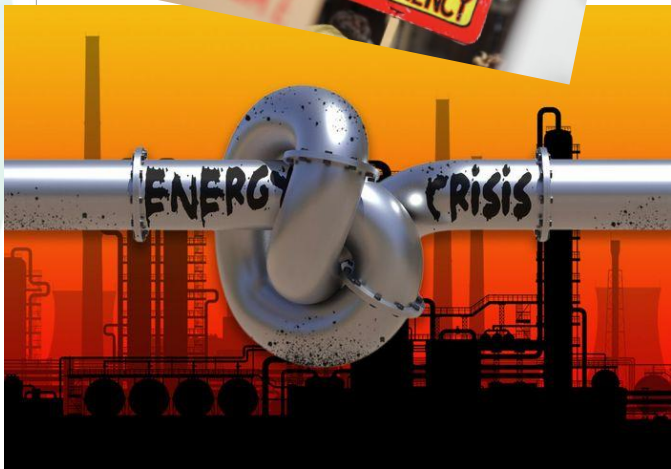
Last two years has seen an unprecedented amount of activity

<u>Carbon Neutral Aspirations</u> the main driver

Role of Radio Spectrum Policy to help combat Climate Change







The Energy Trilemma

Trying to maintain the balance

The Telecoms Challenge

EUTC

Utilities need a combination of radio technologies and frequency bands to complement existing radio and wire-borne technologies of:

- **Fibre (utility owned & commercial)**
- **Copper (PSTN & pilot cables buried with electricity cables and gas pipes)**
- **PLC and BPL which use the power cables themselves for communications**

BUT we do need radio, and … Spectrum Access is the critical factor

Noting that the amount of spectrum required by utilities will not have any impact on public broadband

EUTC Spectrum Proposal

Within Europe, multiple small allocations within harmonised bands:

LESS INTENSE APPLICATIONS

- **VHF spectrum (50-200 MHz)** for resilient voice comms & distribution automation for rural and remote areas. [2 x 1 MHz]

ANCHOR BAND

- **UHF spectrum (400 MHz bands)** for SCADA, automation, smart grids and smart meters. [2 x 3 MHz]

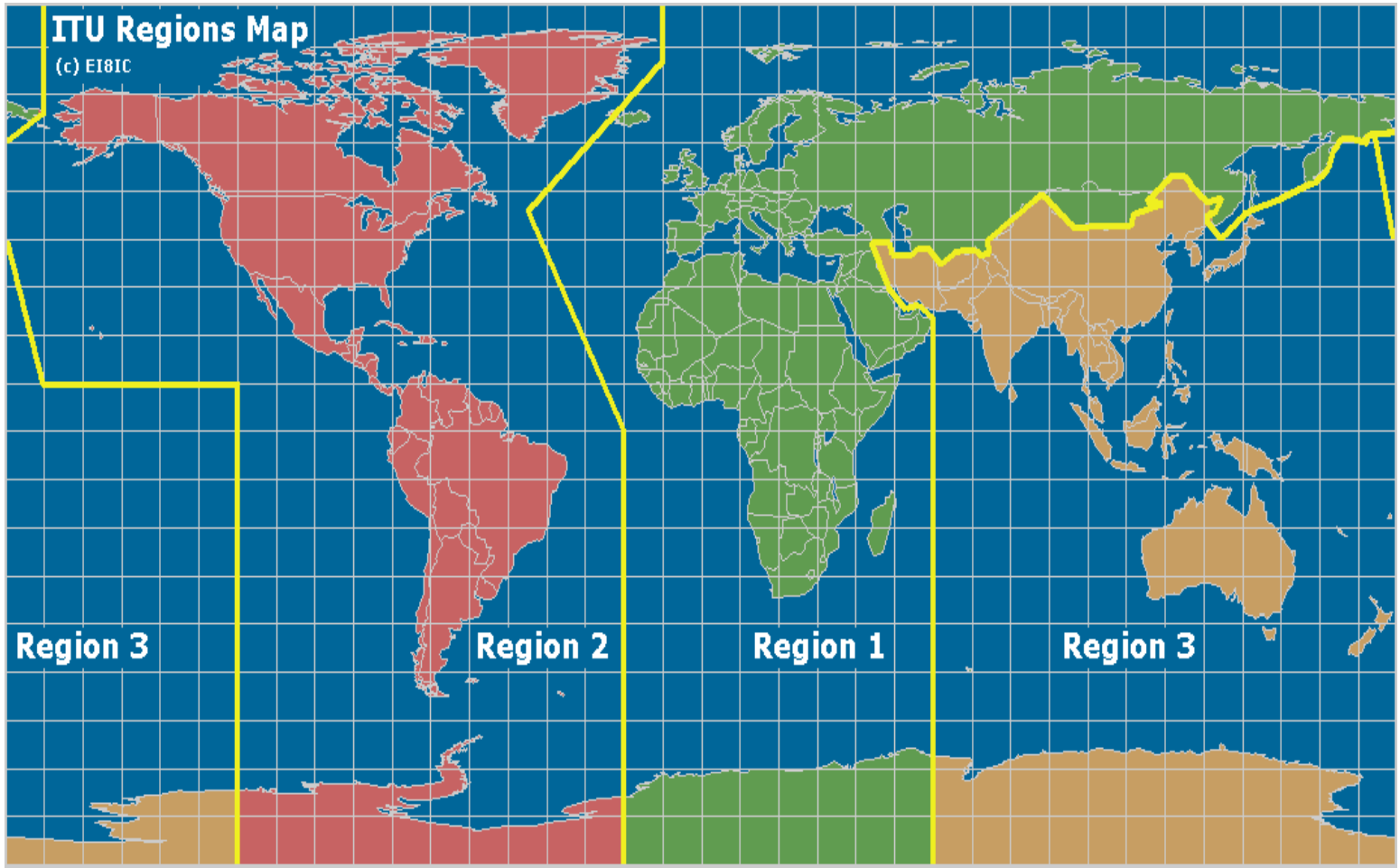
MORE DENSE APPLICATIONS

- **Lightly regulated or licence-exempt shared spectrum** for smart meters and mesh networks. (870-876 MHz)
- **Mid-Band Region (1-5 GHz)** for more data intensive smart grid, security and point-to-multipoint applications. [10 MHz]

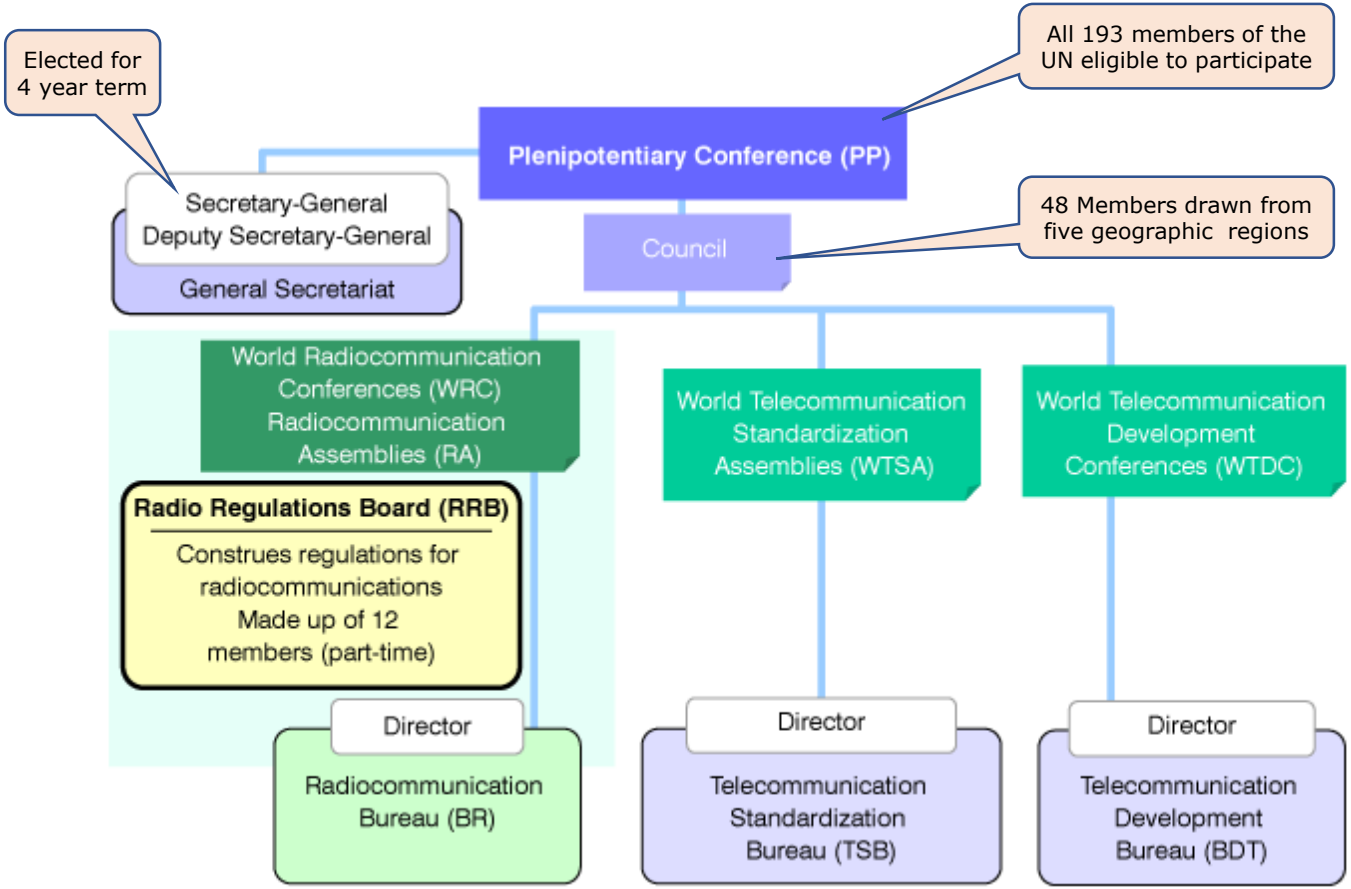
FOUNDATION BANDS

- **Public microwave bands (1500 MHz – 58 GHz)** for access to utilities' core fibre networks/strategic resilient back-haul.
- **Public satellite bands** to complement terrestrial services for particular applications.

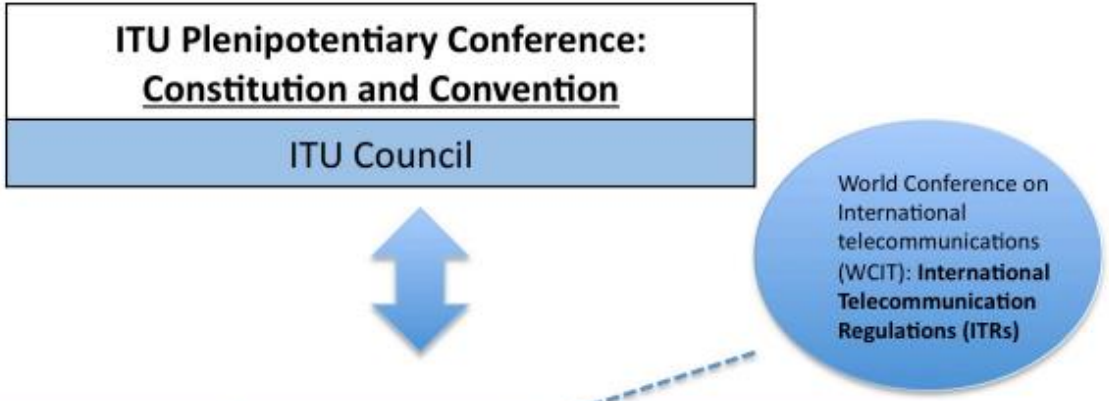
Spectrum Management at a Global Level



Spectrum Management at a Global Level



Spectrum Management at a Global Level

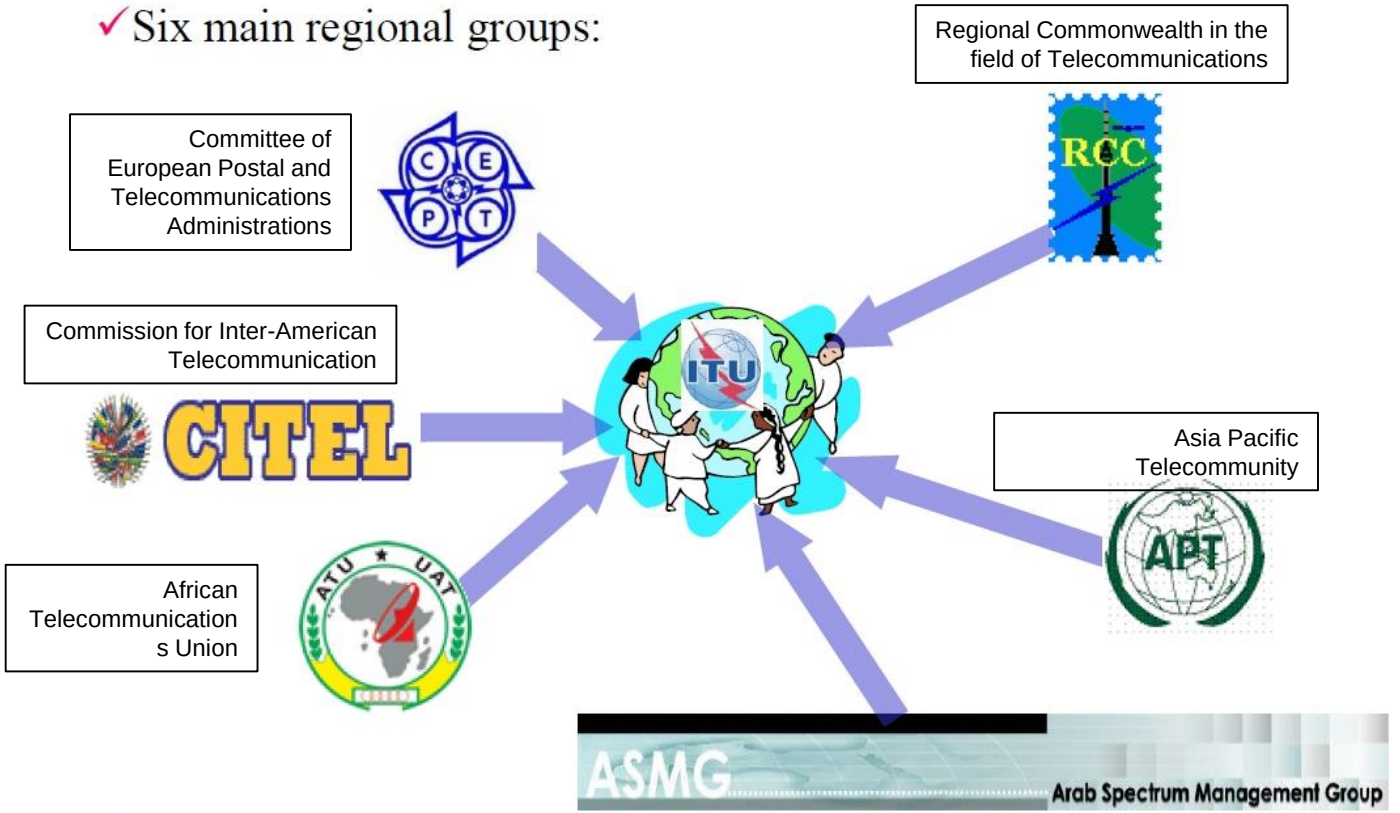


ITU-R	ITU-T	ITU-D
World Radio Conference (WRC): Radio Regulations	World Telecommunication Standardization Assembly (WTSA)	World Telecommunication Development Conference (WTDC)
Radio Advisory Group (RAG)	Telecommunication Standardization Advisory Group (TSAG)	Telecommunication Development Advisory Group (TDAG)
Study Groups	Study Groups	Study Groups

Spectrum Management at Regional Level

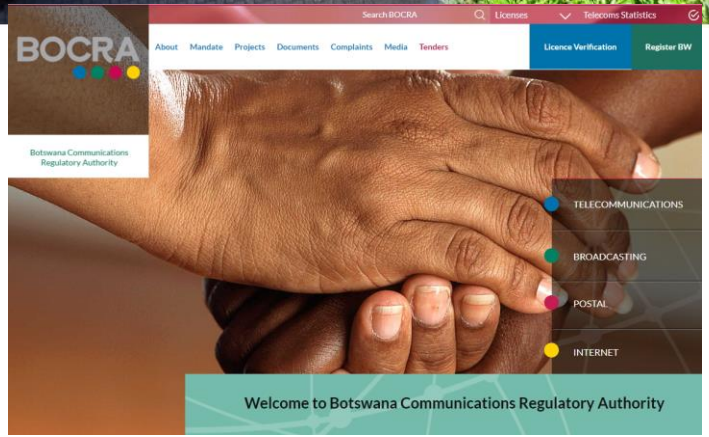
EUTC

✓Six main regional groups:



✓For the preparation of common and coordinated proposals

Spectrum Management at Regional Level

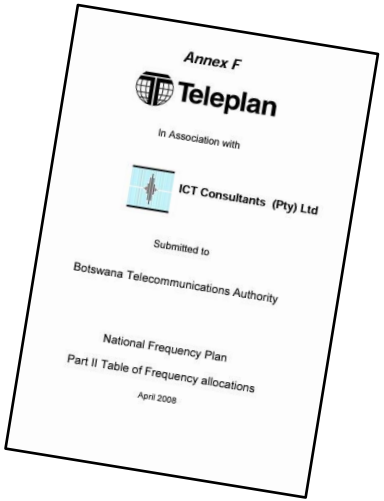


WHO WE ARE!

AFRICAN TELECOMMUNICATIONS UNION

Founded in 1977 as a specialized agency of the Organisation of African Unity, now African Union, in the field of telecommunications, the African Telecommunications Union (ATU-UAT) took its present name in 1999. This led to the transformation of the agency into a partnership between public and private stakeholders in the Information and Communication Technology (ICT) sector.

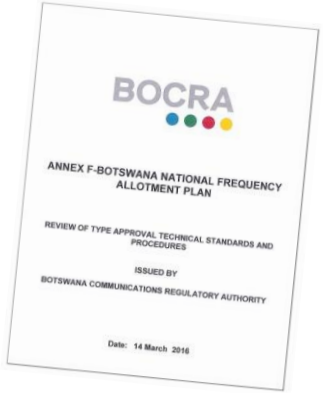
READ MORE



Spectrum Management at National Level

National Radio Frequency Plan - BTA

Frequency bands (MHz)	ITU Region 1 Radio Regulations	National Allocations	Main Utilisations in Botswana	Frequ. bands Mid Frequ. (MHz)	Duplex bands (MHz)	Remarks
450 - 455	*FIXED* *MOBILE ADD 5.XXX* *5.209 5.271 5.286 5.286A 5.286B 5.286C 5.286D 5.286E*	*FIXED* *MOBILE* *5.209 5.286 5.286A*	*FIXED* *LAND MOBILE*	452.000 – 453.000 450.000 – 452.000 453.000 – 453.975 453.975 – 454.425 454.425 – 459.000	462.000 – 463.000 460.000 – 462.000 463.000 – 463.975 464.425 – 469.000	FX 6, 10 MHz duplex ML 4, 10 MHz duplex ML 5, 10 MHz duplex Paging ML 6, 10 MHz duplex 450 – 470 MHz identified as suitable for rural services (NTELETSA) using FDD technology with 10 MHz duplex distance
455 - 456	*FIXED* *MOBILE ADD 5.XXX* *5.209 5.271 5.286A 5.286B 5.286C 5.286E*	*FIXED* *MOBILE* *5.209 5.286A*	*FIXED* *LAND MOBILE*	454.425 – 459.000	464.425 – 469.000	ML 6, 10 MHz duplex 450 – 470 MHz identified as suitable for rural services (NTELETSA) using FDD technology with 10 MHz duplex distance
456 – 459	*FIXED* *MOBILE ADD 5.XXX* *5.271 MOD 5.287 5.288*	*FIXED* *MOBILE*	*FIXED* *LAND MOBILE*	454.425 – 459.000	464.425 – 469.000	ML 6, 10 MHz duplex 450 – 470 MHz identified as suitable for rural services (NTELETSA) using FDD technology with 10 MHz duplex distance
459 – 460	*FIXED* *MOBILE ADD 5.XXX* *5.209 5.271 5.286A 5.286B 5.286C 5.286E*	*FIXED* *MOBILE* *5.209 5.286A*	*FIXED* *LAND MOBILE*	459.000 – 460.000		FBML 4 450 – 470 MHz identified as suitable for rural services (NTELETSA) using FDD technology with 10 MHz duplex distance


BOCRA

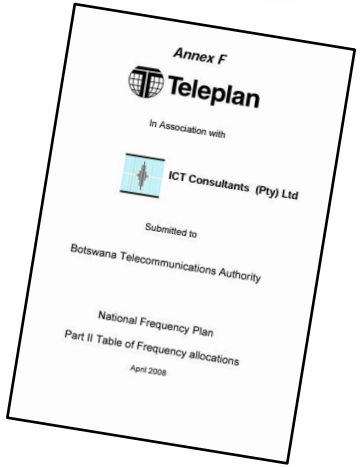
ANNEX F-BOTSWANA NATIONAL FREQUENCY ALLOTMENT PLAN

REVIEW OF TYPE APPROVAL TECHNICAL STANDARDS AND PROCEDURES

ISSUED BY

BOTSWANA COMMUNICATIONS REGULATORY AUTHORITY

Date: 14 March 2016


Annex F

Teleplan

In Association with

ICT Consultants (Pty) Ltd

Submitted to

Botswana Telecommunications Authority

National Frequency Plan

Part II Table of Frequency allocations

April 2008

Spectrum Management at National Level

National Radio Frequency Plan - BTA

Frequency bands (MHz)	ITU Region 1 Radio Regulations	National Allocations	Main Utilisations in Botswana	Frequ. bands Mid Frequ. (MHz)	Duplex bands (MHz)	Remarks
460 – 470	*FIXED* *MOBILE ADD 5.XXX* *Meteorological-Satellite (space-to-Earth)* *MOD 5.287 5.288 5.289 5.290*	*FIXED* *MOBILE* *Meteorological-Satellite (space-to-Earth)* *5.289*	*FIXED* *LAND MOBILE* *Meteorological-Satellite (space-to-Earth)*	462.000 – 463.000 469.000 – 470.000 460.000 – 462.000 463.000 – 463.975 463.975 – 464.425 464.425 – 469.000	452.000 – 453.000 450.000 – 452.000 456.000 - 460.000 454.425 – 469.000	FX 6, 10 MHz duplex FX 7 FB 4, 10 MHz duplex FB 5, 10 MHz duplex Low power devices, mobile radios FB 6, 10 MHz duplex 450 – 470 MHz identified as suitable for rural services (NTELETSA) using FDD technology with 10 MHz duplex distance
470 – 790	*BROADCASTING* *5.149 5.291A 5.294 5.296 5.300 5.302 5.304 5.306 ADD 5.311 5.312*	*BROADCASTING* *5.149 5.304 5.306 5.311*	*BROADCASTING (terretsrial)*	470.000 – 790.000		Television band IV/V Channel 21-60. ST61 Support functions for broadcasting

Equipment Availability at a Global Level

EUTC

3GPP A GLOBAL INITIATIVE

ETSI

IEEE Advancing Technology for Humanity

Shaping the future

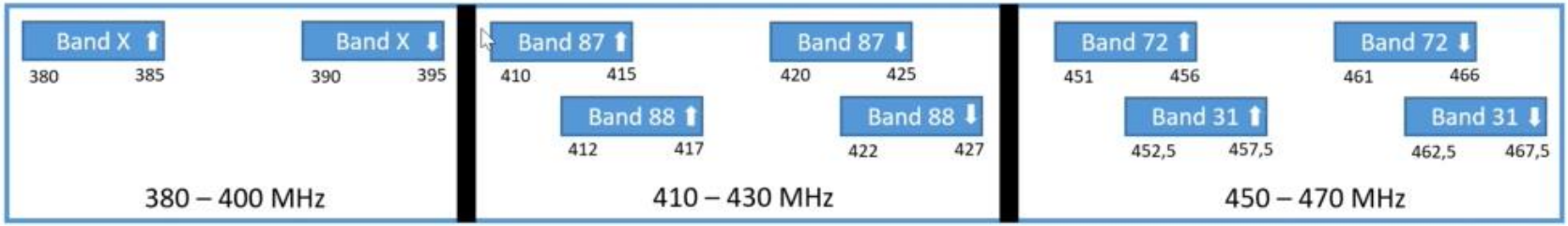
The 3rd Generation Partnership Project (3GPP) unites seven telecommunications standard development organizations, known as Organizational Partners', providing their members with a stable environment to produce the Reports and Specifications that define the 3GPP system.

ARIB atis CCSA ETSI tsdsi TTA TTC

Equipment Availability at a Global Level

LTE Bands currently in scope of the WG S+R

450 alliance.org
promoting the advancement of 450 MHz worldwide.



Roadmap towards a new or updated 3GPP standard:

1. Submit a Work Item to 3GPP
2. Formalise equipment standards (ETSI)
3. Spectrum assignments by national administrations

Typically 3 – 5 years

On the Raodmap: new LTE Band at 380 – 400 MHz and 5G for the existing bands

Spectrum Allocation at a Global Level

EUTC

The battle for the 6 GHz band

	Wi-Fi Frequency Bands		
	2.4 GHz	5 GHz	6 GHz
802.11ax	←	→	→
802.11ac		↔	
802.11n	←	→	
802.11g	←	→	
802.11a		↔	
802.11b	←	→	
802.11be		↔	→

Proposals

Wi Fi 5 · Wi Fi 6 · Wi Fi 6E CERTIFIED · 7

Down to 5030 MHz — License - exempt

5G NR - Licensed

5G NR-U (5G New Radio – unlicensed) & *WiFi 6E*

5G NR-U (unlicensed) & from 2022 *WiFi 6E*
Low Power Indoor & Very Low Power portable

UK considering Low Power *WiFi 6E*

5945 MHz — 7070 MHz — 7075 MHz

Current plan

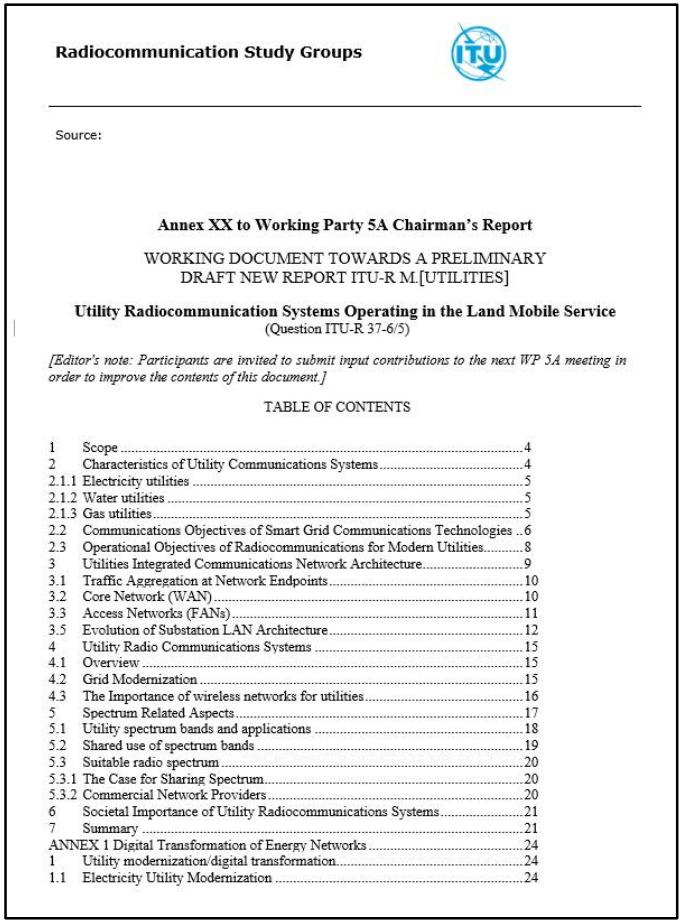
Fixed satellite (Earth to space)

Lower 6GHz (500 MHz)
Fixed microwave links

Upper 6GHz (700 MHz)
Fixed microwave links

5925 MHz — 6425 MHz — 7125 MHz

Spectrum Allocation at a Global Level



Radiocommunication Study Groups

Source:

Annex XX to Working Party 5A Chairman's Report

WORKING DOCUMENT TOWARDS A PRELIMINARY
DRAFT NEW REPORT ITU-R M.[UTILITIES]

Utility Radiocommunication Systems Operating in the Land Mobile Service
(Question ITU-R 37-6/5)

[Editor's note: Participants are invited to submit input contributions to the next WP 5A meeting in order to improve the contents of this document.]

TABLE OF CONTENTS

ITU-R Working Party 5A

Draft Report on Utility Radiocommunications Systems seeking recognition at international level of the importance of spectrum access for Smart Grid Applications.

Global Challenges of Spectrum Access for Smart Grid Applications

1st December 2022

Botswana

Adrian Grilli

Technical Manager

European Utility Telecoms Council

Brussels

www.EUTC.org

EUTC.org/resources/

EUTC

Agenda

Nigel working life has Several decades of experience in operational telecoms, In his previous digital journey Nigel worked at Nortel , Cisco , Huawei , and now working at Nokia

***Digitalisation of Energy with 5G Secure Communications for low carbon grid transformation*, Nigel Nawacki,** NOKIA

Energy Utility Digital Industry CX CTO at Nokia EU/UK

EVOLUTION

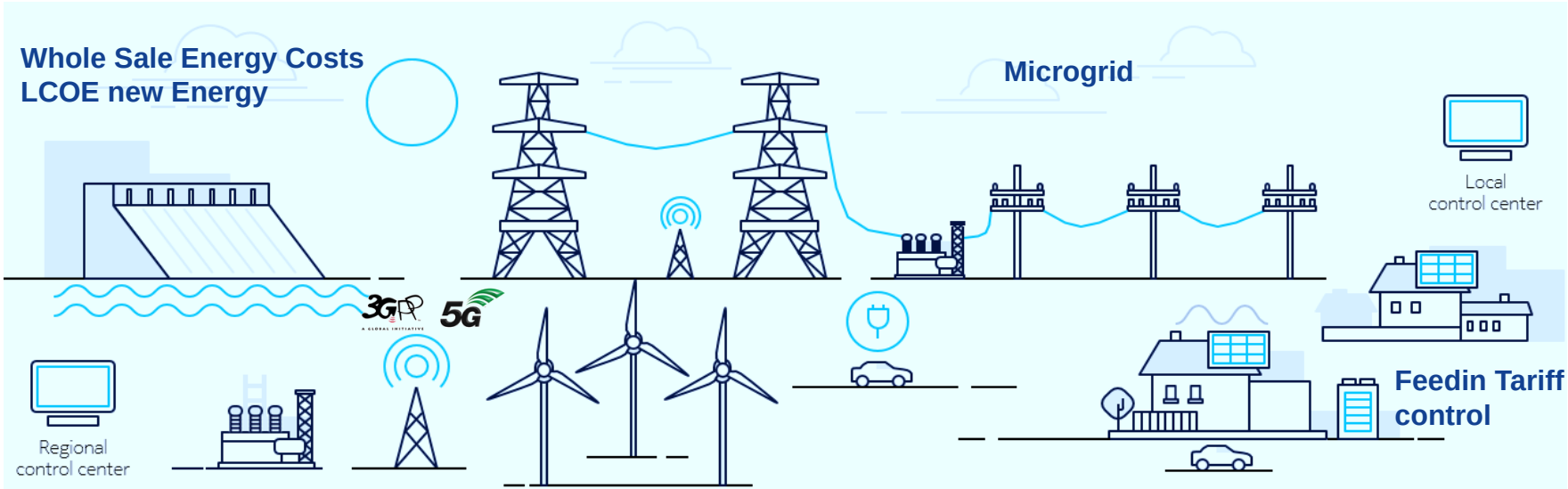
Digitalisation of Energy
5G Secure Communications for low carbon grid transformatio

Nigel Nawacki - CX CTO Energy Utilities - Nokia

1st December, 2022

Systemically - immense challenges building the Low / Zero Carbon grid

Pressing need to introduce autonomy/integrity/automation/optimization/securit



NOKIA

Agenda

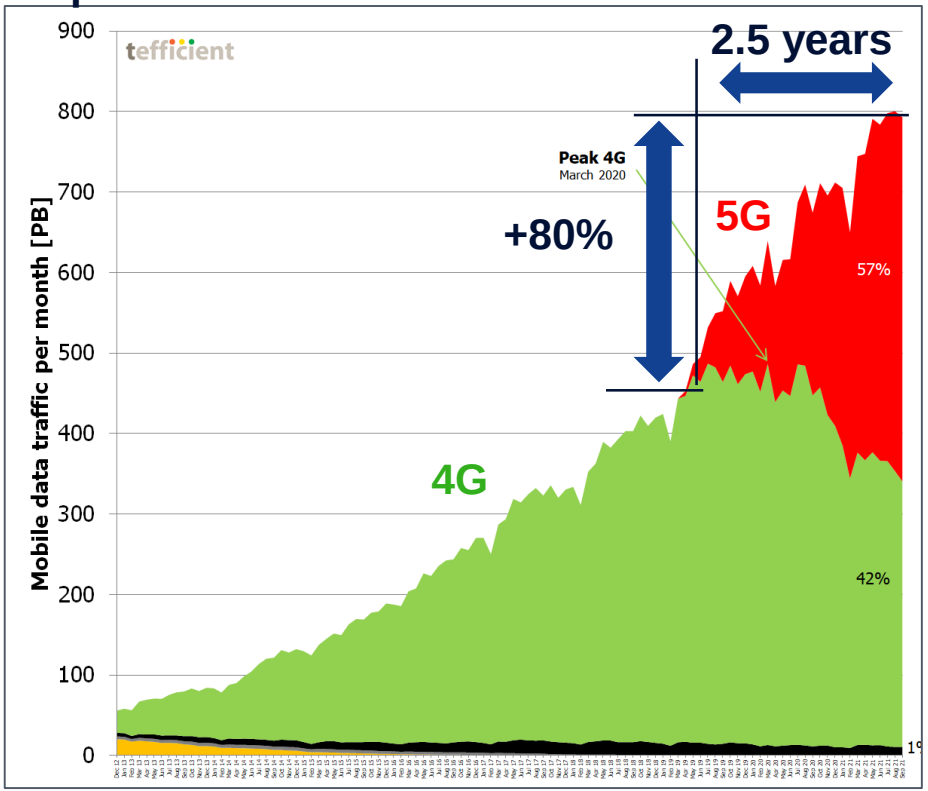
5G – Fundamentals and Parallels (a Recap)

5G – Use case samples for the Secure - Low carbon operating Grid

Conclusions to draw ….

5G Traffic Growth – Learnings

September 2021



- 5G carries 57% of data in less than 2.5 years
- 4G traffic started to decline during 2021
- Data growth accelerated after 5G launch
- Data growth +80% after 5G launch which corresponds to 10x traffic in 10 years
- Improved Energy efficiency of cellular infrastructure – and virtualised core.

Pervaisive Communications

Net Zero Targets

Accelerated Energy Needs (Macro Forces

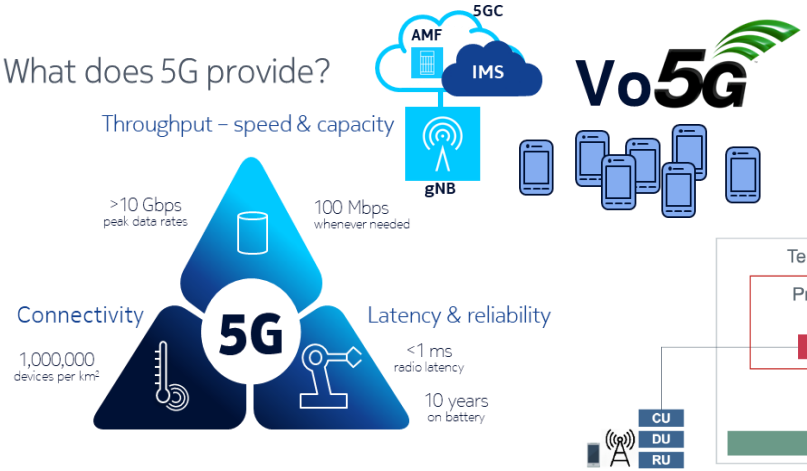
Improved Energy Regulations

European NETZERO Targets – 2030+

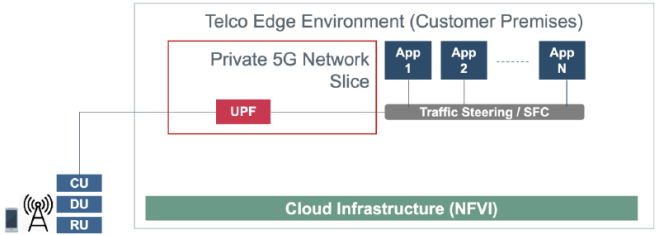
NOKIA

Digitalisations of energy - 5G Essentials

- Enhanced mobile broadband,
- Massive machine-type communications,
- Ultra-reliable and low latency communications.



Bandwidth is a quantity measure of data moving (measured in X bits per second) and **latency** is a measure of the delay end end (measured in milliseconds). bandwidth = “seats” latency = “speed”



- **AMF: Access and Mobility management Function**
- **SMF: Session Management Function**
- PCF: Policy Control Function
- AUSF: Authentication Server Function
- NSSF: Network Slice Selection Function
- UDM: Unified Data Management
- UDR: Unified Data Repository
- NRF: Network Repository Function
- **NEF: Network Exposure Function**

Certificate Management is Key

But its not just improved throughput and speed, Improved **Physical Uplink Control Channel (PUCCH)** and other new features improve the responsive nature of the radio fabric compared to 4G (EPC + eNB)

Improved Trust Model for UE and Network via new Authentication functions (5G was designed with Security)

= More devices per cell site , improved Security features , Utilisation , Simplification (eSIM)

Industry Evolution

Grid / Substation Evolution

Unidirectional flow of power

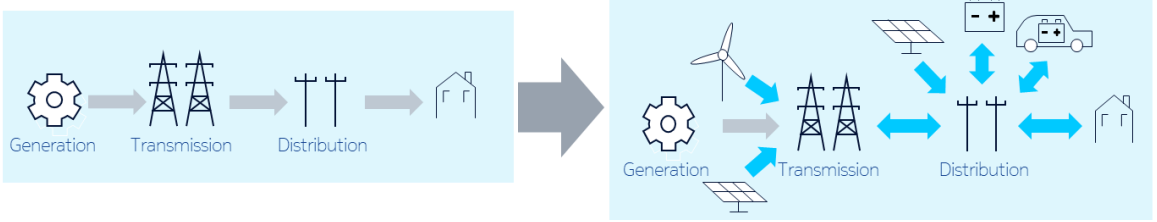
Climate Change unconsicous

Fixed Pricing

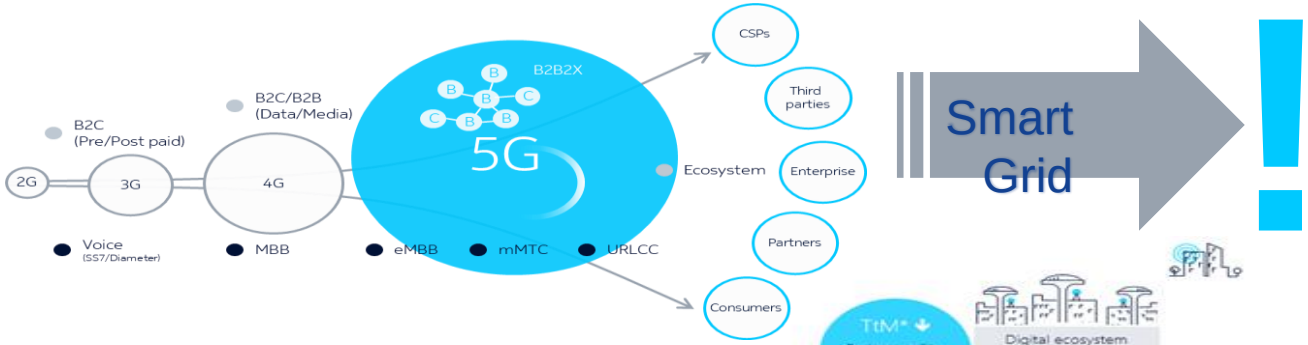
Distributed, multiple power sources

Climate change demands increased efficiency

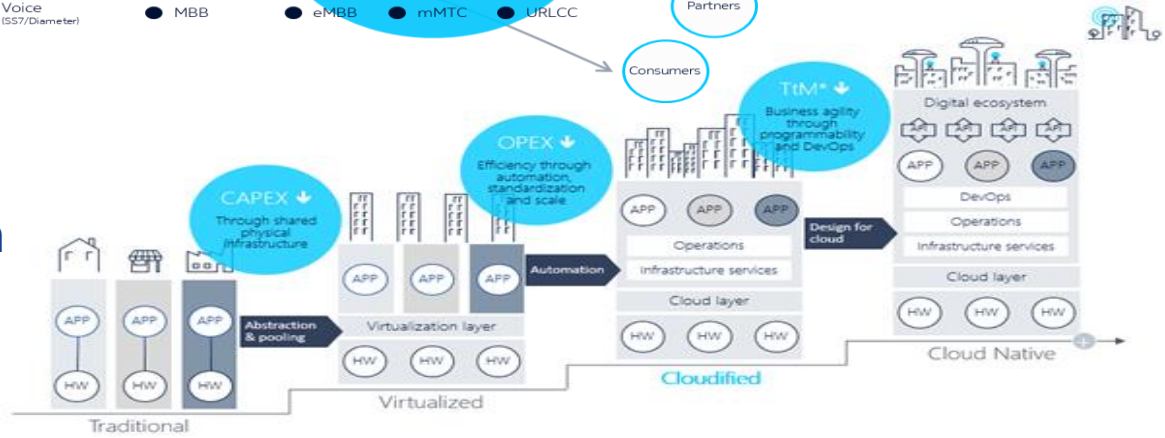
Dynamic Pricing More competitive and stringent regulatory environment



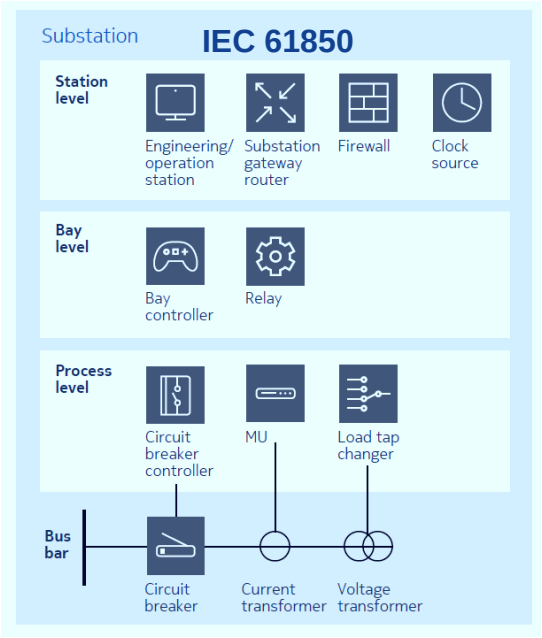
Telco Evolution

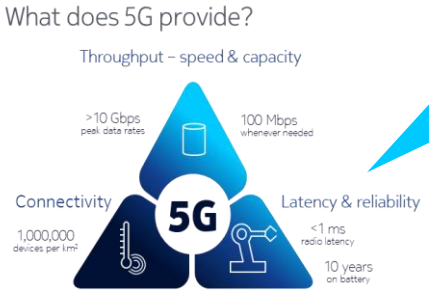


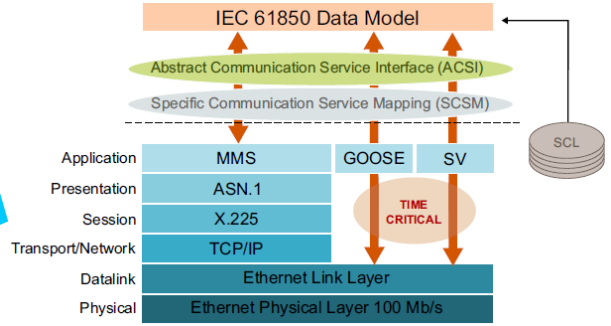
Cloudification Evolution



Digital Substation – 5G Evolution







3rd Generation Partnership Project;
Technical Specification Group Services and System Aspects;
Study on 5G Smart Energy and Infrastructure (Release 18)

- **Interoperability** among electrical equipment vendors, enabling a multivendor environment and fostering and accelerating grid innovations
- **Consolidation of multiple networks into one converged network**, both inside and outside the substation
- **Deployment of a cost-effective Scaling** network replacing tons of copper wire at the process level for significant cost saving (material and installation), improved safety security and abundant bandwidth for new innovations.

GOOSE/MMS

SV

1588v2

Message Type	Example Application	Time Constraint
1A—Fast messages, trip	**Circuit breaker commands and states (GOOSE)**	**≤3 ms**
1B—Fast messages, other	The same as above	≤20 ms
2—Medium speed messages	RMS values calculated from type 4 messages	≤100 ms
3—Low speed messages	Alarms, non-electrical measurements, configurations	≤500 ms
4—Raw data messages	**Digital representation of electrical measurement (SV)**	**≤3 ms**
5—File transfer functions	Files of data for recording settings	≤1000 ms
6—Time synchronization messages	**IED internal clock synchronization**	**none**

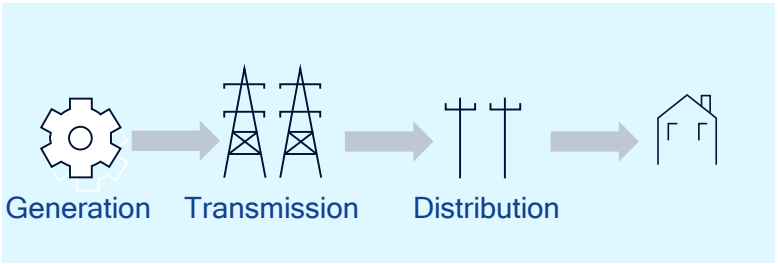
Smart Grid Communications

Transformation to “Low Carbon – Distributed Future Grid”

Unidirectional flow of power

Climate Change unconsicous

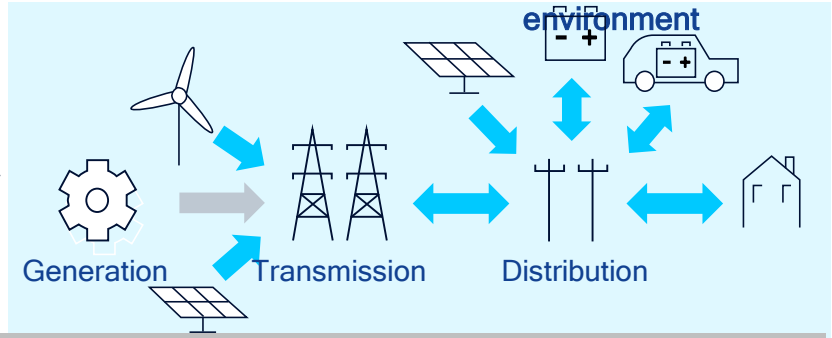
Fixed Pricing



Distributed, multiple power sources

Climate change demands increased efficiency

Dynamic Pricing
More competitive and stringent regulatory environment



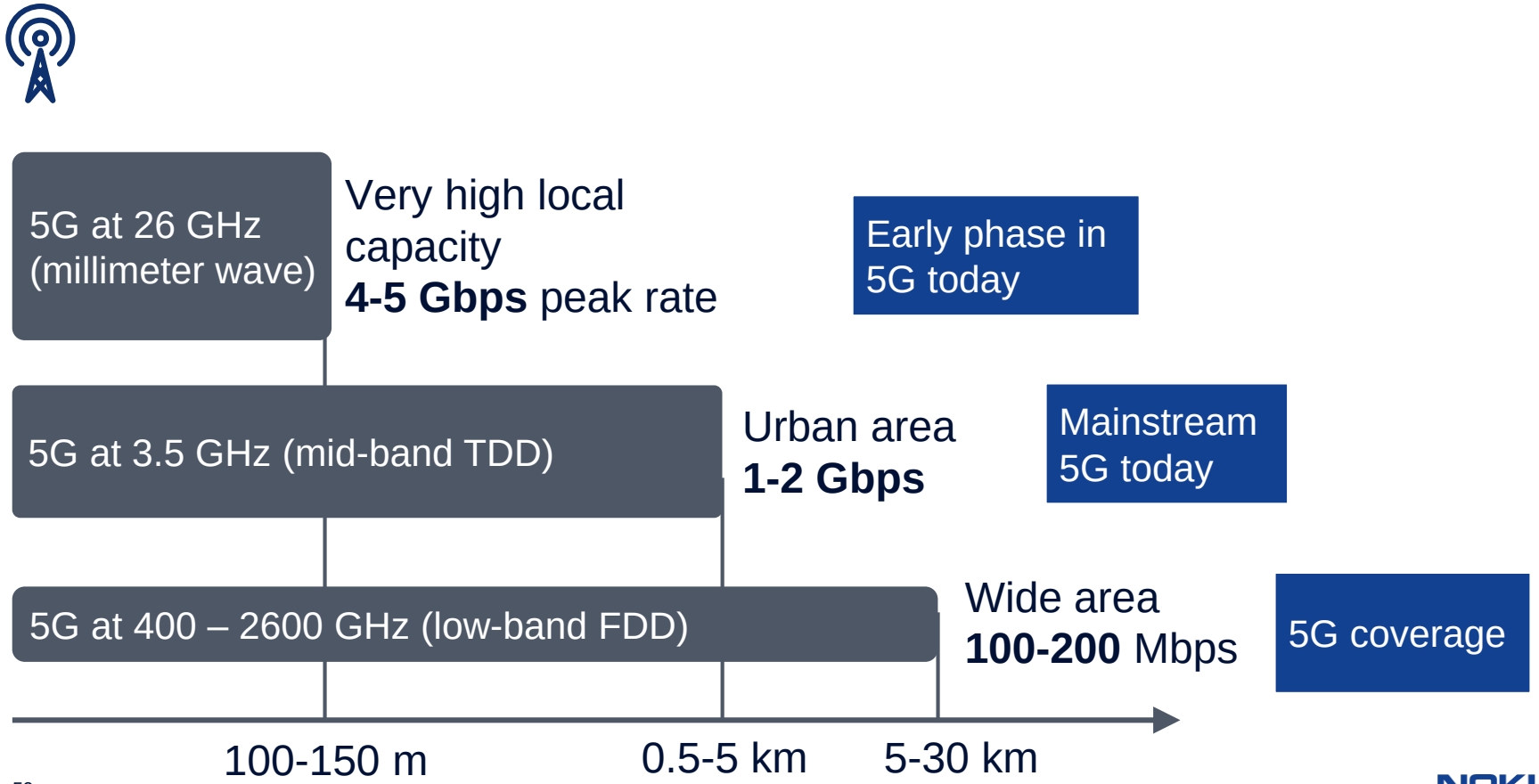
5G ENABLING THE SHIFT

Control of the decentralized network of renewable, intermittent power sources through a reliable wireless network with guaranteed latency

Improve the reliability, safety, availability, efficiency of power grid through communications. Current approach is fiber between nodes with DWDM and IP/MPLS; distance between relays determined by delay constraint,

Difficulty connecting Secondary Substation and Distributed Assets

5G Spectrum Reach and Range –Low and High Bands



NOKIA

Agenda

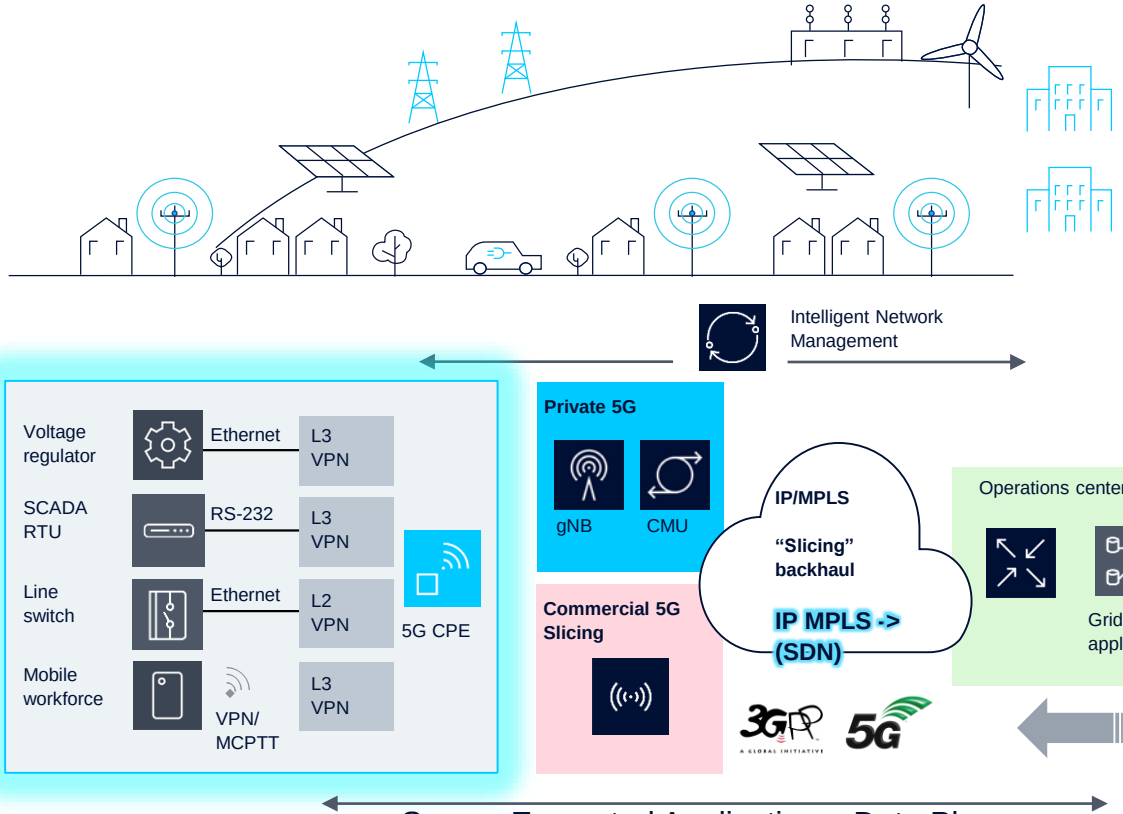
5G – Fundamentals and Parallels (a Recap)

5G – Use case samples for the Secure - Low carbon operating Grid

Conclusions to draw ….

5G Low Carbon Grid

Foundation of a safer and more reliable grid



Utility benefits:

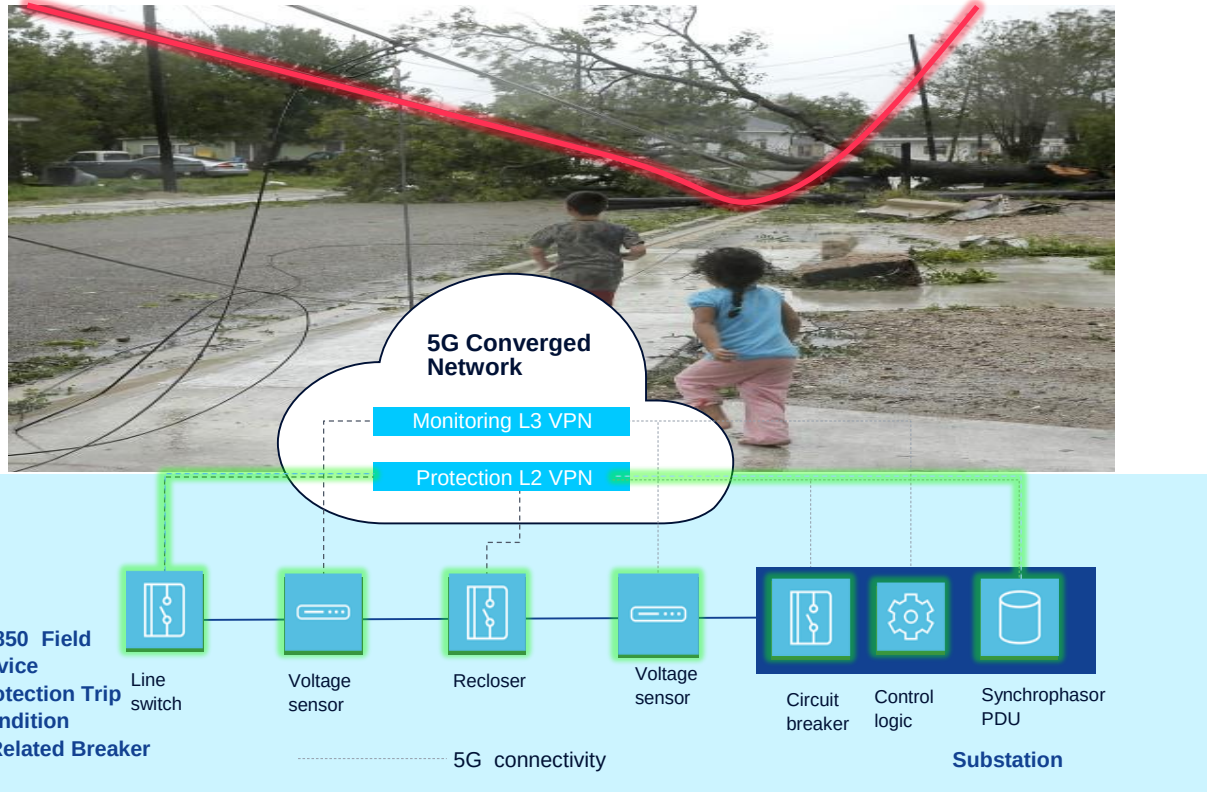
- Heightened grid monitoring
- Strengthened power reliability
- Improved fire prevention from falling wire
- Reduced OPEX
- Faster On Board – Grid Supply Points

Solution highlights:

- Converged 5G as a platform for distribution automation
- Strong redundancy by dual-homing with private and commercial 5G networks
- Secure communications Encrypted Source-destination

Use case – improves grid safety

Protecting life and property from falling wire



Fire prevention and public safety by falling copper protection

Utility benefits:

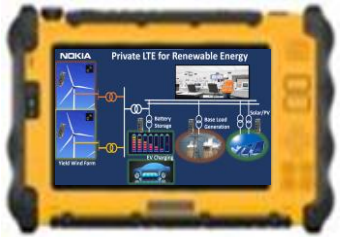
- Improved safety records
- Minimized fire and electric shock hazards

Solution highlights:

- Consistent delay assurances (under 30 mS Ideally) **Millisecond level**
- L2 and L3 VPN solution with delay and delivery assurance
- **Local Compute autonomy**

Field crew wireless connectivity

Facilitate information sharing with Control Room



Field 5G / AR VR

Utility benefits:

- Increase worker productivity
- Quicker problem diagnosis
- Reduced Truck roles
- Improved Situational Awareness

Solution highlights:

- 5G hot spot
- Backhaul over Secure 5G
- **AR / VR brings control room to front office**

Today - Two Options (Combo) for Ultra Reliable Low Latency Communication (URLLC)

Option 1: PUBLIC networks slicing

- Guaranteed quality with slicing
- Example cases: public safety, remote control of machinery

09.04.2020 14:00

Elisa chosen as the sole radio network supplier to Finland's new public safety network for 10 years due to quality and coverage

John Deere Continues to Push the Boundaries of 5G and Agriculture

Option 2: Dedicated PRIVATE network

- Dedicated local network
- Example case: private LTE at Helsinki airport or 5G at Kittilä gold mine

Agnico Eagle to deploy underground and surface 5G network with Telia, Digita and Nokia at Kittila gold mine in Finland

Posted by Paul Moore on 13th October 2021

NOKIA

Agenda

5G – Fundamentals and Parallels (a Recap)

5G – Use case samples for the Secure - Low carbon operating Grid

Conclusions to draw ….

5G-Advanced Timing in 3GPP

R15 Extreme mobile broadband

R16 Industrial IoT (URLLC)

R17 Wider ecosystem expansion

R18 5G Advanced

2019 | 2020 | 2021 | 2022 | 2023 | 2024

Release 15
- Mobile broadband
- Commercial 04/2019

Release 16
- Industrial IoT (URLLC)
- Completed 12/2020

Release 17
- Wider ecosystem
- Completion mid-2022

Release 18
- 5G-Advanced
- Expected 1Q-2024

Metaverse Future with AR and VR

Mark Zuckerberg
12 t ·

FOUNDER'S LETTER, 2021

5G ADVANCED + Meta = Future Utility Worker

In this future, you will be able to teleport instantly as a hologram to be at the office without a commute, at a concert with friends, or in your parents' living room to catch up. This will open up more opportunity no matter where you live. You'll be able to spend more time on what matters to you, cut down time in traffic, and reduce your carbon footprint.

Think about how many physical things you have today that could just be holograms in the future. Your TV, your perfect work setup with multiple monitors, your board games and more -- instead of physical things assembled in factories, they'll be holograms designed by creators around the world.

You'll move across these experiences on different devices -- augmented reality glasses to stay present in the physical world, virtual reality to be fully immersed, and phones and computers to jump in from existing platforms. This isn't about spending more time on screens; it's about making the time we already spend better.

NOKIA

The evolution will require industry collaboration and investment

Examples only	5G (2021)	5G-Advanced	6G era (2030)
Video	High quality video (4K-8K)	**XR for Utilities - fully immersive** user experience possible with uLLC	Holographic transmissions **Back Office / Front Office** Meta Sphere
Digital – Physical Confluence	Object Driven Digital Twinning (e.g. an engine)	Large Scale Digital Reconstruction (e**.g. Compute and Local Autonomy)**	Broad based digital twins with **real-time synchronous updates**
Localization and sensing	Data communication and control	Provide precise location and timing services that complement GNSS	Network with a 6th sense **Synchronicity**

Key Conclusions

- 5G – A Standards based approach to underpin entire Low Carbon system(S)
- Complete synergy with IEC 61850 objectives
- Security / high availability is integral to architecture/ featurettes
- TRL is high for radio components and emerging REDCAP chipsets (IOT speak for 5G)
- What is not to like ?

Thank You

NOKIA


NOKIA

Agenda

Welcome & Opening, Jacqueline Redmond/ Federico Coffele/Kinan Ghanem,

Cor *nges in smart grid: the importance of validation*, James Irvine

Glo

Digi

Nawacki,

Chris has been involved in Sync & Timing since the early 1990s - from E1 clock recovery cards to Atomic Clocks and GNSS Timing Systems for critical infrastructure. Chris has solid experience in supporting the deployment, operation and upgrade of timing systems across a wide range of end-use cases.

***Sync and Timing for secure Critical Infrastructure*, Chris Farrow**

Technical Services Manager, Chronos Technology Ltd.

Debswana Smart Grid Solution, Karabo Mmokwa

Zero Trust security in OT, Chris McGookin,

Time & Sync for Critical Infrastructure

Christian Farrow

1st December 2022

Time & Sync for Critical Infrastructure

- Intro
- Time as an enabler
- GNSS, O-RAN & 5G as Attack Surface expanders
- Mitigations
  - GNSS Firewalls and the vPRTC
- Summary

Chronos Technology Ltd

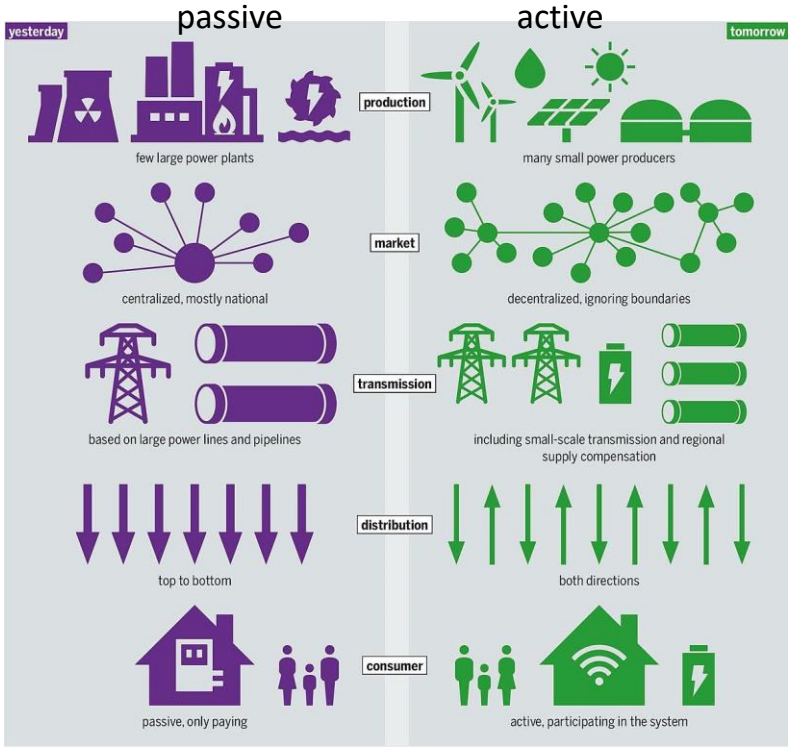
- Founded in 1986 by Professor Charles Curry
- Owned through Employee Trust
- UK based with 35 employees
- Manufacturer & Reseller
- Contribute to world telecom timing standards
  - ITU Standards Committee (SG15/Q13)
  - International Steering Groups – Timing (ITSF, WSTS) & Navigation (RIN)
- ISO9001:2015 Accredited

Chronos: Our Business

- Resilient Synchronisation & Timing Solutions
- GNSS (GPS and other Satellite Based Services) Vulnerability & Mitigation Solutions
- Professional Services
- Markets
  - Telecom / Cable
  - Power
  - Financial Services
  - Defence & Security
  - Law Enforcement
  - Broadcast

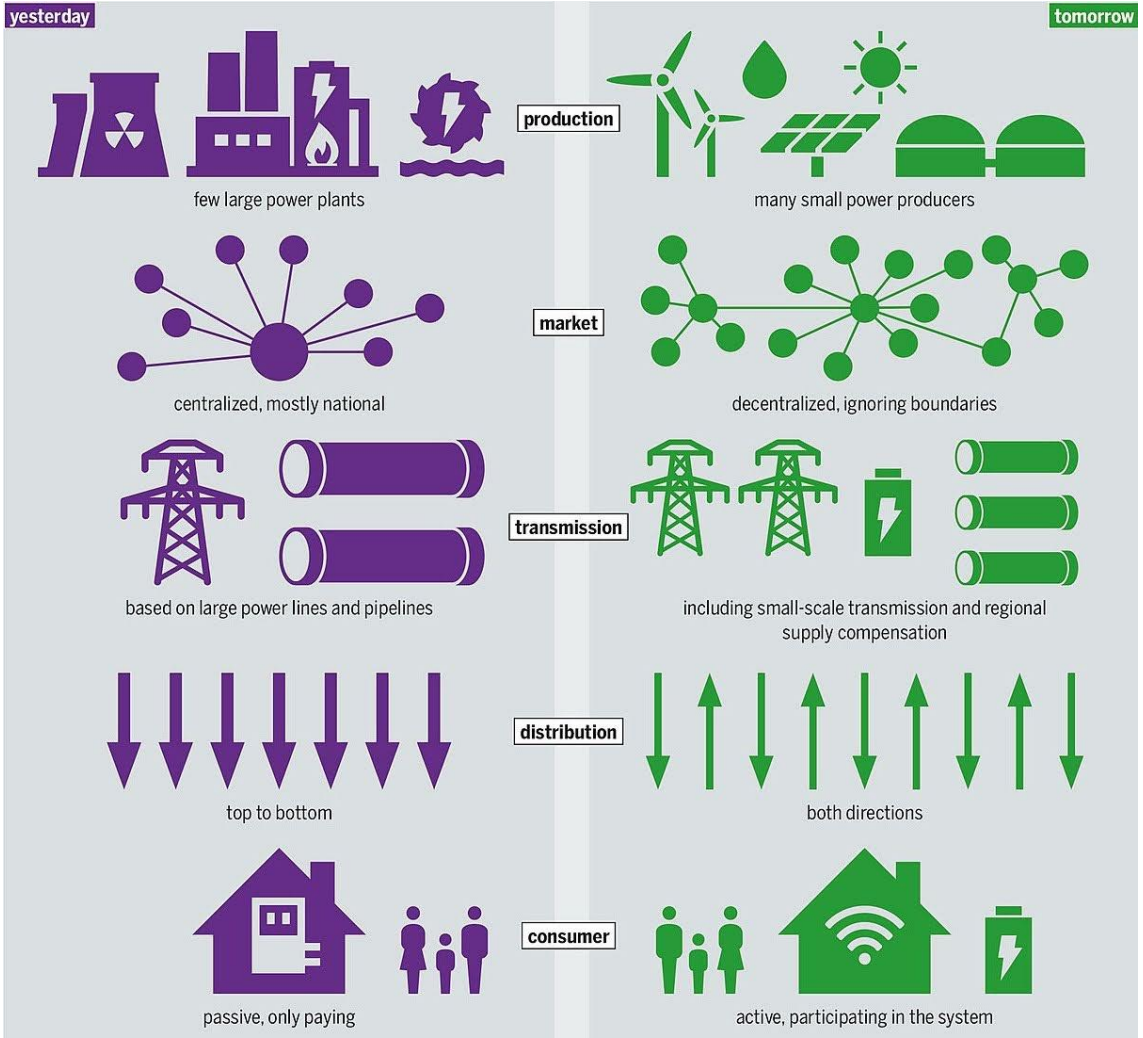
MICROCHIP

The Smart Grid



- From a few “permanently spinning machines” with inertia to many + new generation technologies
- Diversification of energy sources/storage
- Uni- to Bi-directional energy flow
- More dynamic/reactive
- Smart cells: Brokers/Agents buying/selling energy with autonomous dis/connection
- De-carbonisation of transport (EVs)

Bartz/Stockmar: https://energytransition.org/2018/04/europe-must-choose-a-green-future/



- But where do we need sync?

  (as before)
  Syncro-phasors, Sampled values
  Fault detection/location
  IEC61850 Digital Substation (PTP)

- Grid-tie inverters, synchronverters, metering
  Smart broker/agent

- Moving from focus on 50Hz machines to adding DC/AC conversion

Security

- Physical Access controls are extensive
- Private or Isolated networks

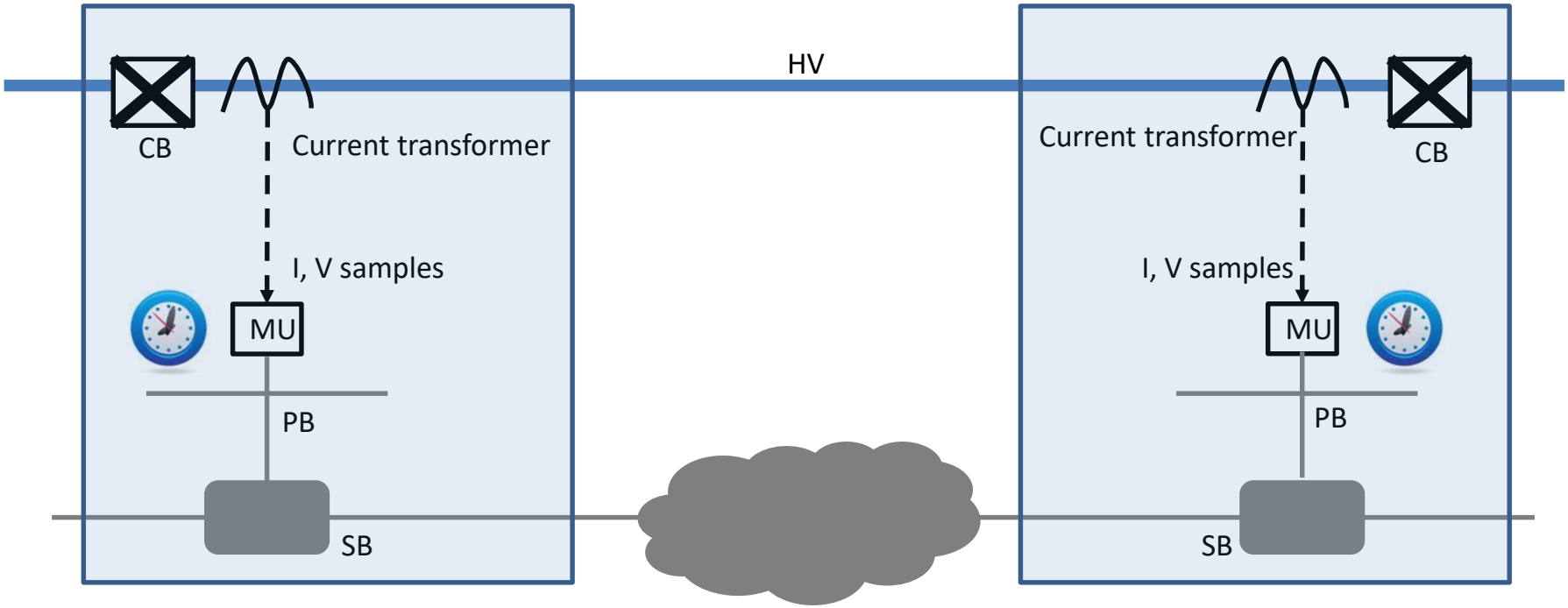
- …but

Security

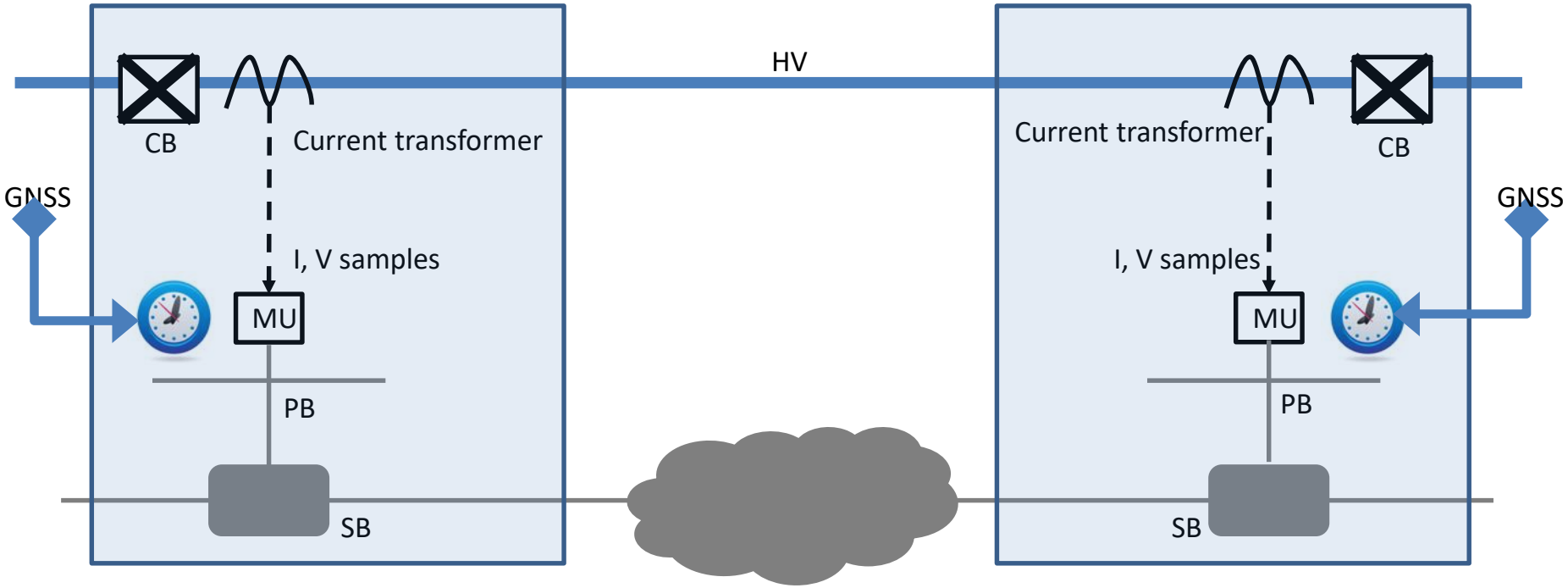
- Physica
  are ext
- Private

- …but

Application: fault detection in Power Distribution

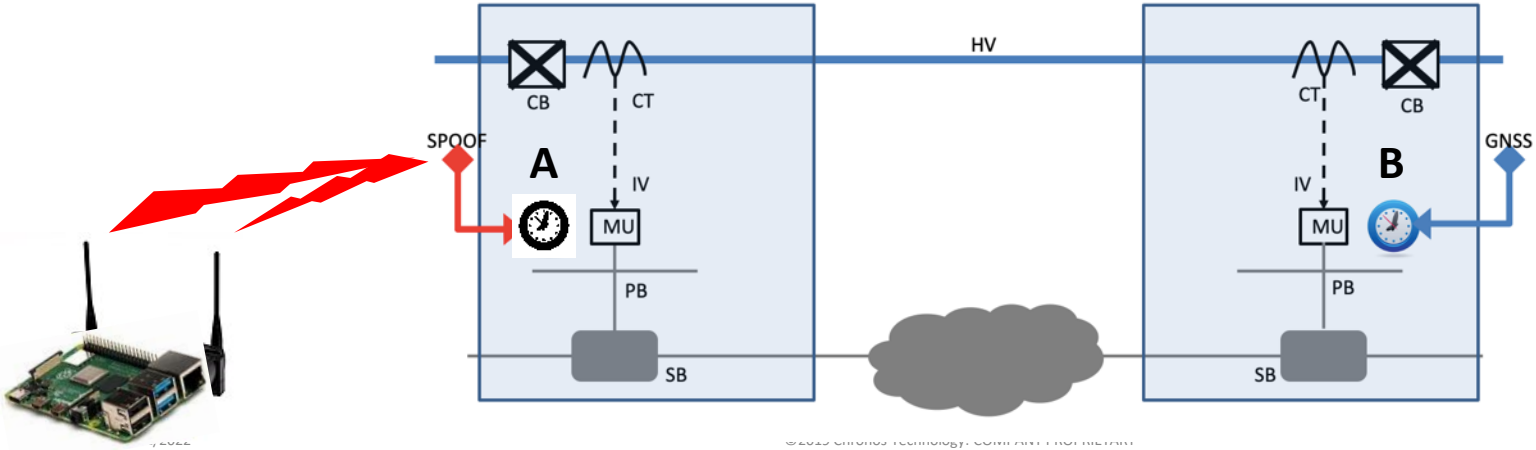


Power Distribution threat: time as attack vector



Power Distribution threat: time as attack vector

- An attacker armed with a GNSS spoofer could remotely corrupt the time at location A
- Causing errors in measured values between location A and B
- Causing fault reports or incorrect shut-downs of network areas



Local GNSS receiver

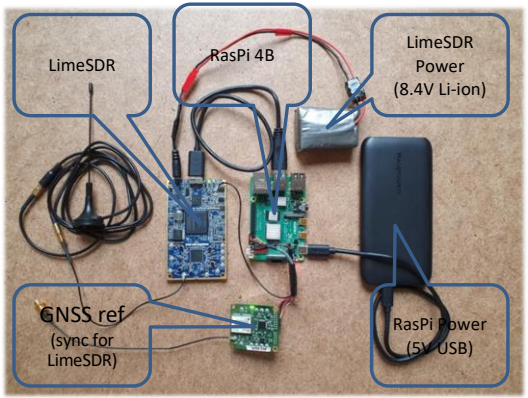
- Jamming/Spoofing now civilian activities

Jamming now a civilia

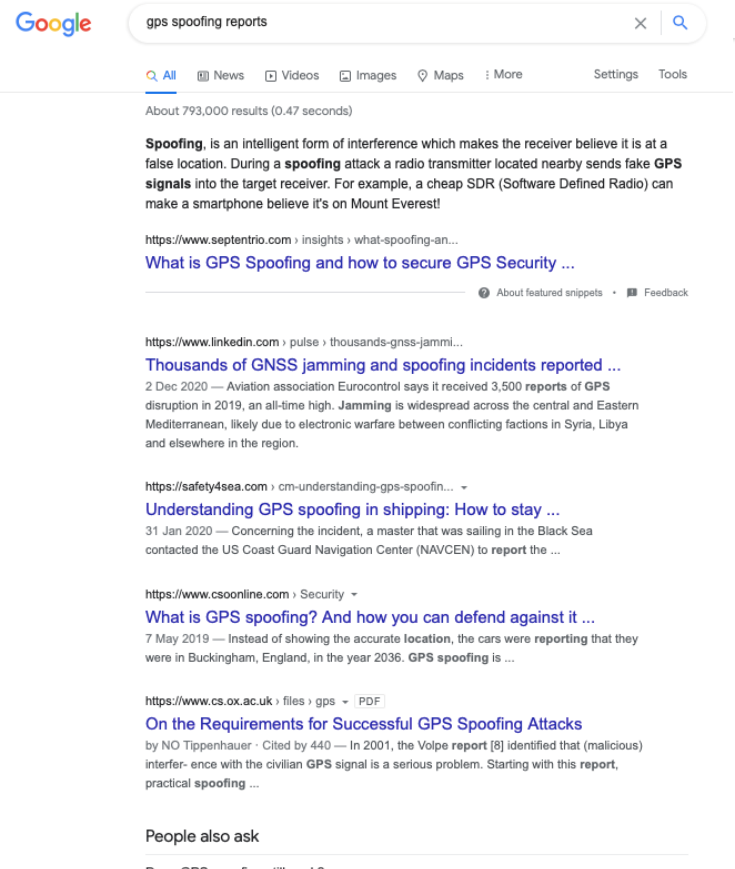
- Privacy concerns have lead to an Jammers”
  - Business/Fleet vehicle tracking
  - Offender tracking
  - Freight Tracking
  - High-value cars fitted with tracker
  - “Privacy Jammers” for sale on the
    - Some also jam GSM/3G/4G/WiFi/B
  - Personal privacy – criminal activity

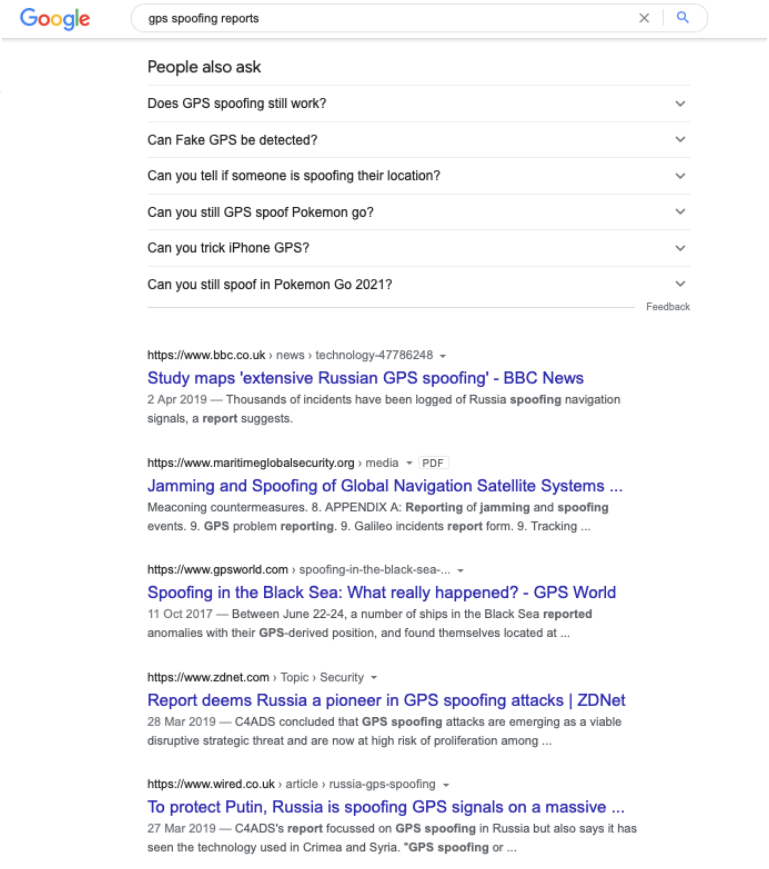
Spoofing now a civilian activity

- Spoofing now trivial with COTS hardware & open-source software
  - Raspberry Pi + SDR + github code + electronics
- Increased use of location services has lead to widespread awareness of “Location Spoofing” techniques
- Of the receivers we tested
  - Some failed and needed power off/on reset
  - Some failed catastrophically needed to be re-flashed

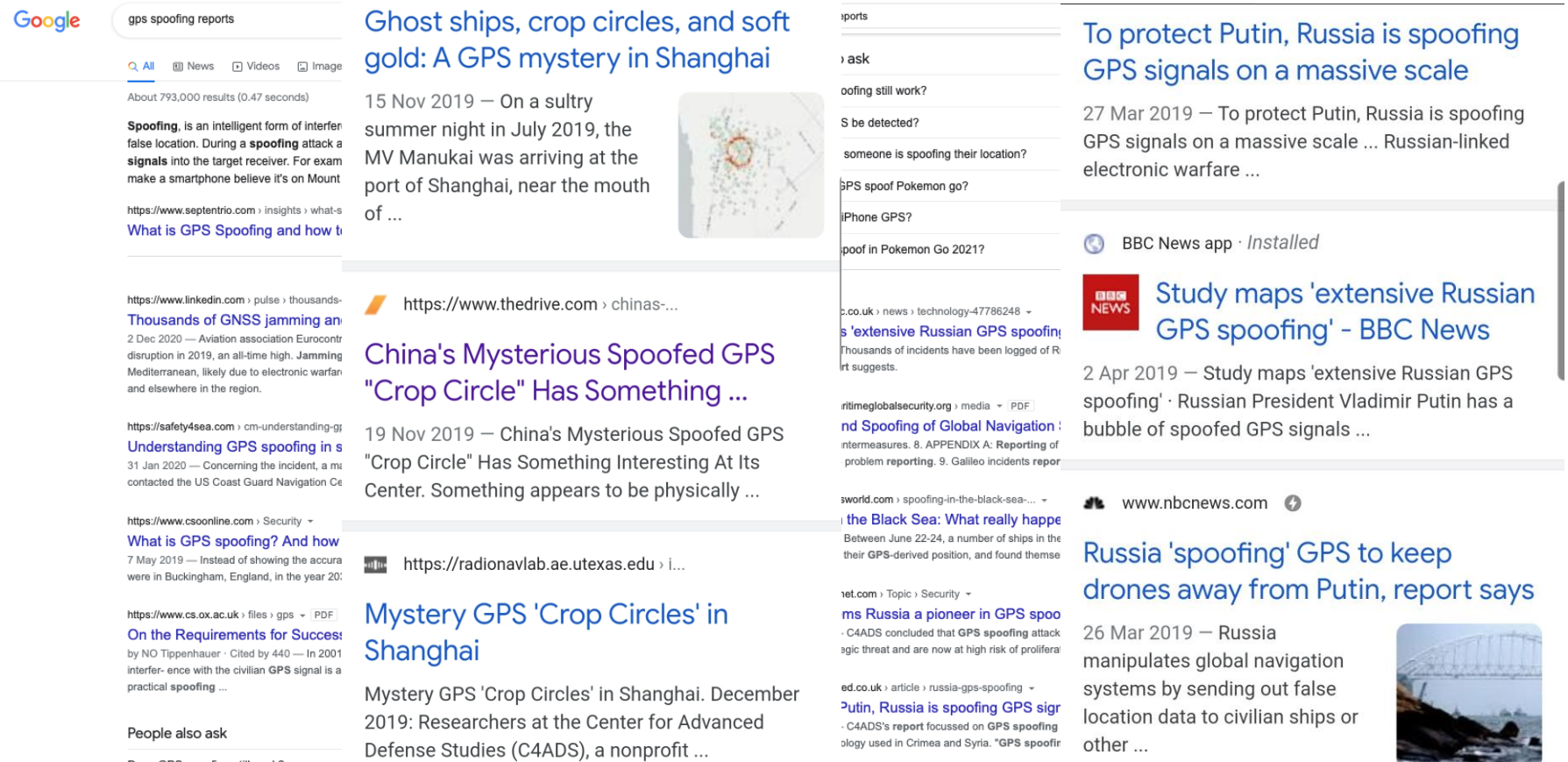


But how common is it?





But how common is it?



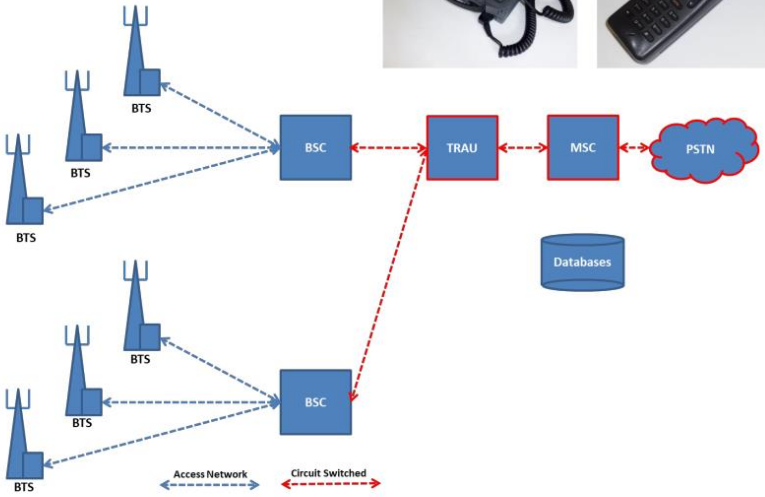
The Transition to Smart Grid Technologies

- 4G & 5G are candidates for networking/remote-telemetry/IoT
- Industry 4.0 along with WiFi 6
- "Private Networks"
  - Self hosted or "Network Slices" of other private/public networks
- "Edge Compute" relies on a backhaul connection

But how do these networks need/use time & sync?

Functional Decomposition of the BTS

GSM network architecture



University of Salford MANCHESTER

10

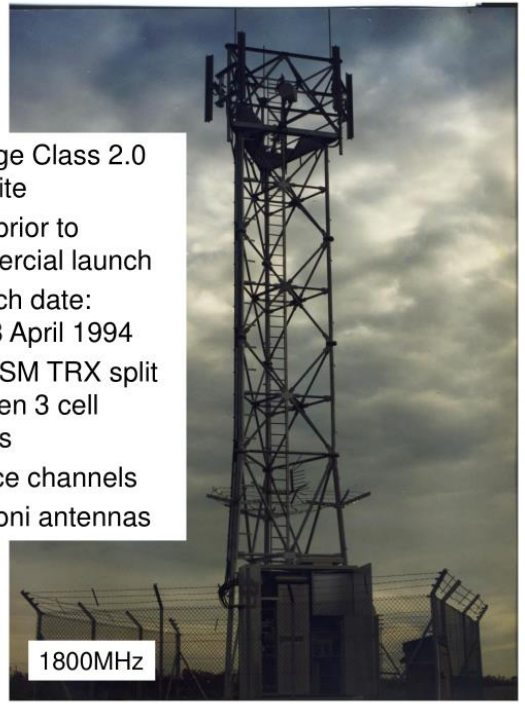
Professor Andy Sutton
@960sutton
www.engagingwithcommunications.com

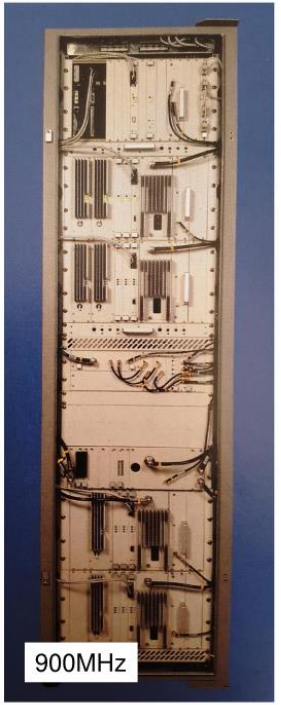
Digital Mobile Network Evolution – from GSM to 5G…

24th October 2019

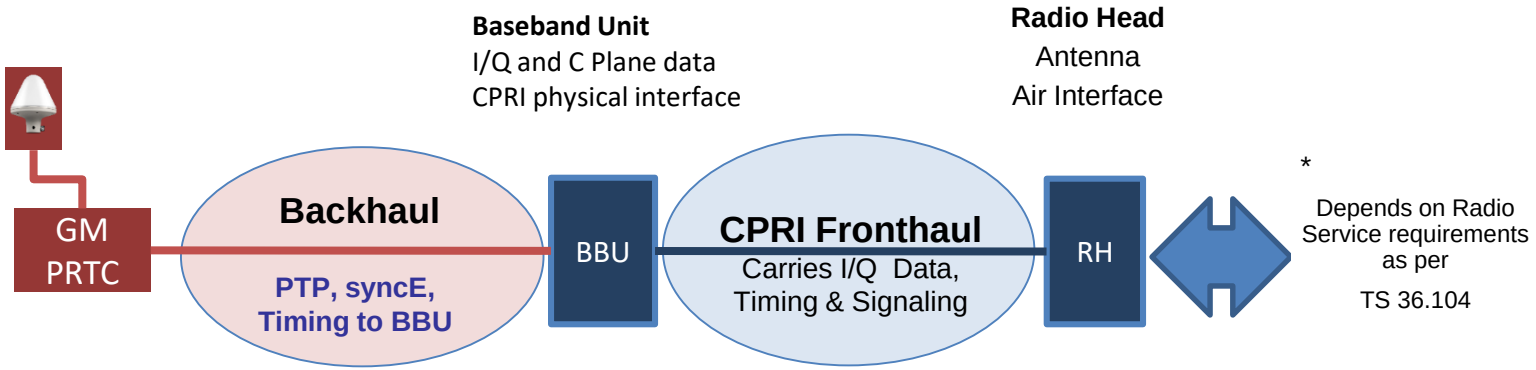
GSM

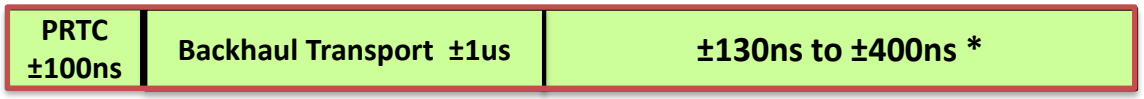
- Orange Class 2.0 BTS site
- Built prior to commercial launch
- Launch date: 28 April 1994
- 1 x GSM TRX split between 3 cell sectors
- 7 voice channels
- Marconi antennas





4G DRAN/CRAN - introducing "fronthaul"



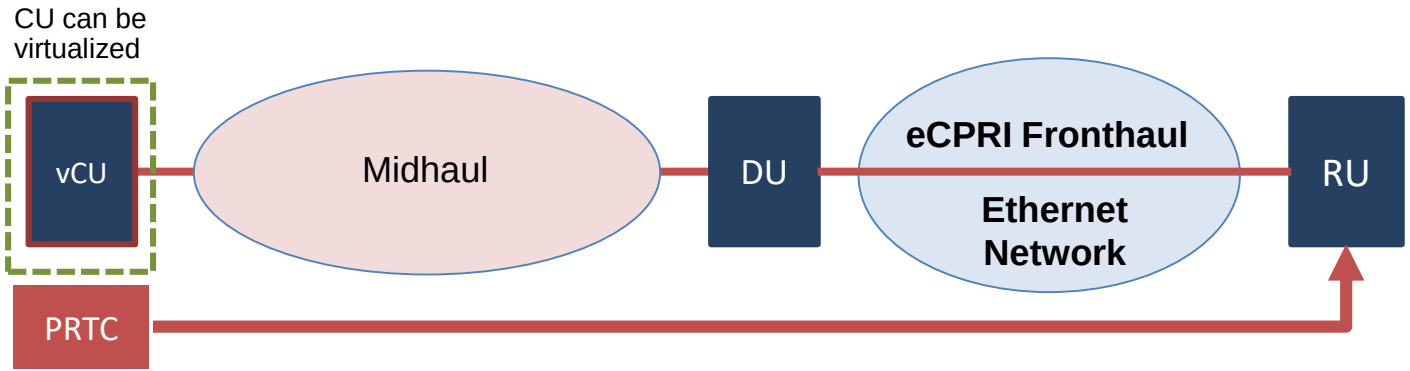


ITU-T TE budget

5G: CU, DU & introducing "midhaul"

BBU is split into 2 functions
CU: Centralized Unit for user data
DU: Distributed Unit for Eth/CPRI phy

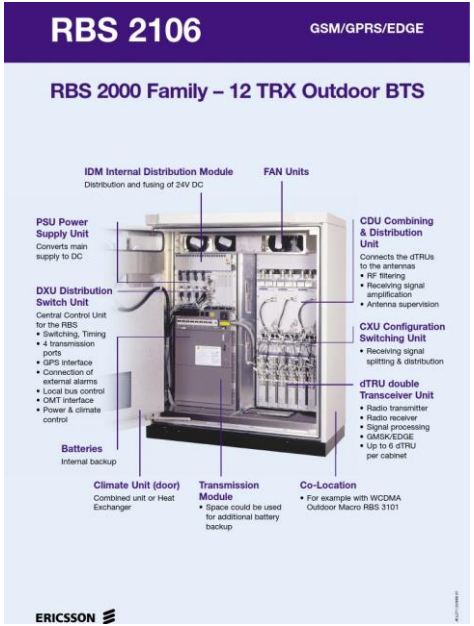
Fronthaul = Ethernet Network
eCPRI carries I/Q data to/from RU
Timing & Signaling outside CPRI

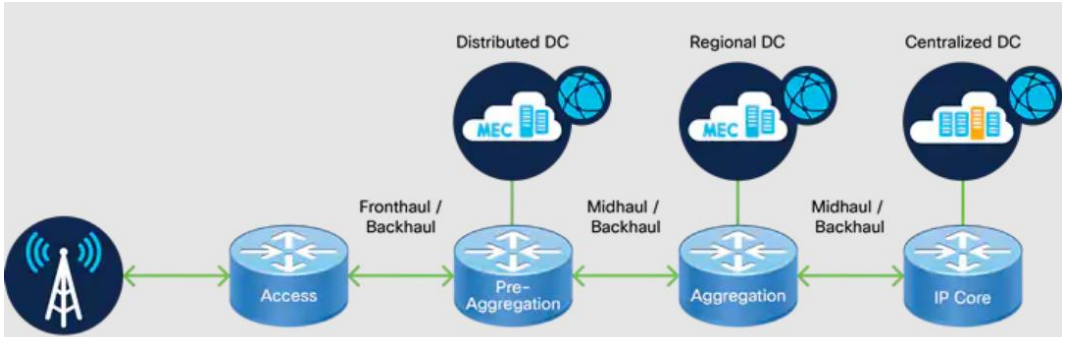


PTP for Timing from PRTC to RU

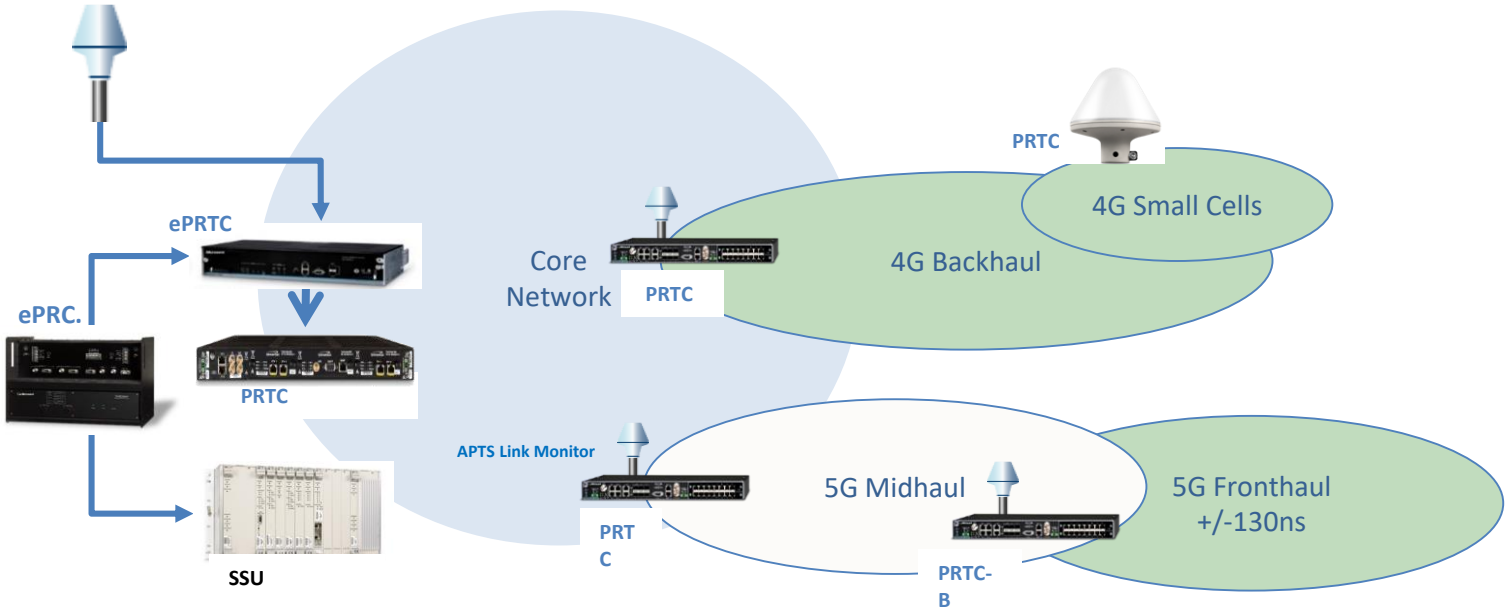
Functional Decomposition of the BTS

- Was:
  - Proprietary hardware & software
- Now:
  - Open Interfaces & COTS Hardware & Software
  - Functionally split over the whole network
    - From the cloud to the furthest edge of the network footprint



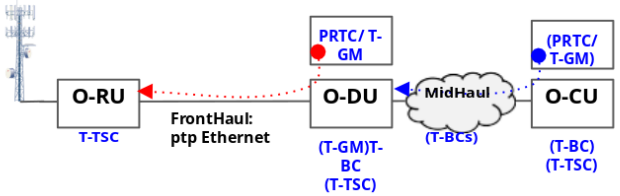


4G/5G Architecture – GNSS attack surface expands



- **LTE-A / 5G Basic Service** **+/-1.5usec**
- **5GNR Advanced Services** **+/-130nsec**

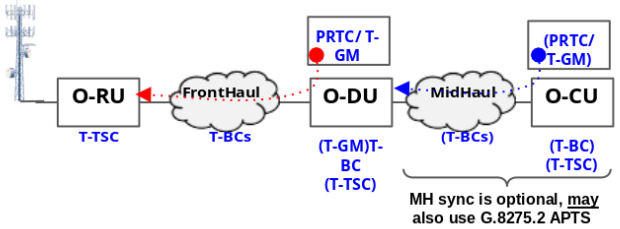
O-RAN “LLS-Cx” Synchronization Reference Configs



WG4 Configuration LLS-C1

FH Direct connection to O-RU(s) from O-DU; sync source in O-DU

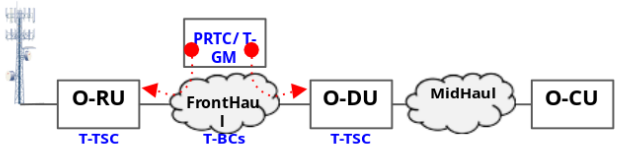
WG9 C1, Option A: GNSS/T-GM Embedded in ~~O-DU~~ (Cloud node)
WG9 C1, Option B: T-GM Directly Connected to O-DU
WG9 C1, Option C: T-GM connected to O-DU via chain of network nodes)



WG4 Configuration LLS-C2

FH Network connection to O-RU(s) from O-DU; sync source in O-DU

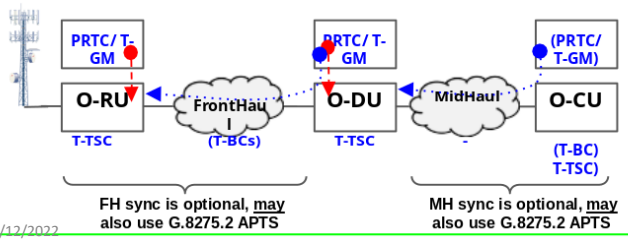
WG9 C2, Opt. A: ~~O-DU~~ (Cloud node) is the nearest common T-BC
WG9 C2, Opt. B: nearest common T-BC not O-DU



WG4 Configuration LLS-C3

Network connection to O-RU from O-DU & sync source in FH network

WG9 C3, Option A: T-GM is the nearest common master
WG9 C3, Option B: nearest common master is not T-GM
WG9 C3, Option C: T-GM in Mid/Back-haul
WG9 C3, Option D: T-GM in Mid/Back-haul with T-BC chain



WG4 Configuration LLS-C4

Network connection to O-RU from O-DU & local sync sources

WG9 C4, Option 1: GNSS at Cell Site (e.g. in O-RU / xNB)
WG9 C4, Option 2: GNSS at Cell & Edge + APTS network

Note:
In clouds, synchronization is part of cloud infrastructure, and decoupled from RAN instances

The Ever Expanding Attack Surface!

Functional Decomposition

- Cloud services – COTS server/networking hardware
  - CVEs – as of 22/11/2022 on https://cve.mitre.org
    - virtual = 30 VM = 756 virtualbox = 332
    - kubernetes = 181 docker = 225 sandbox = 810
      container = 515

- GNSS proliferation
  - Jamming/Spoofing to disrupt "private" networks

Mitigations

01

Protect vulnerable GNSS installations

02

Provide back-up timing signals wherever possible

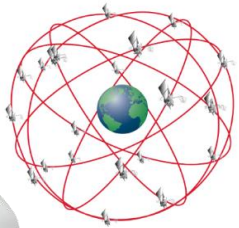
- Network based: NTP/PTP, SyncE

03

Consider owning your own timescale

- Enabled with PRTC, dedicated optical interconnect & HP-BC
- The "vPRTC"

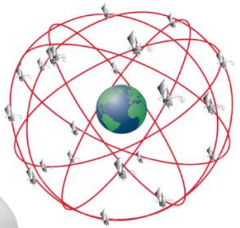
GNSS vulnerability



Live Sky
(not secure)

Existing GNSS receivers

GNSS Firewall

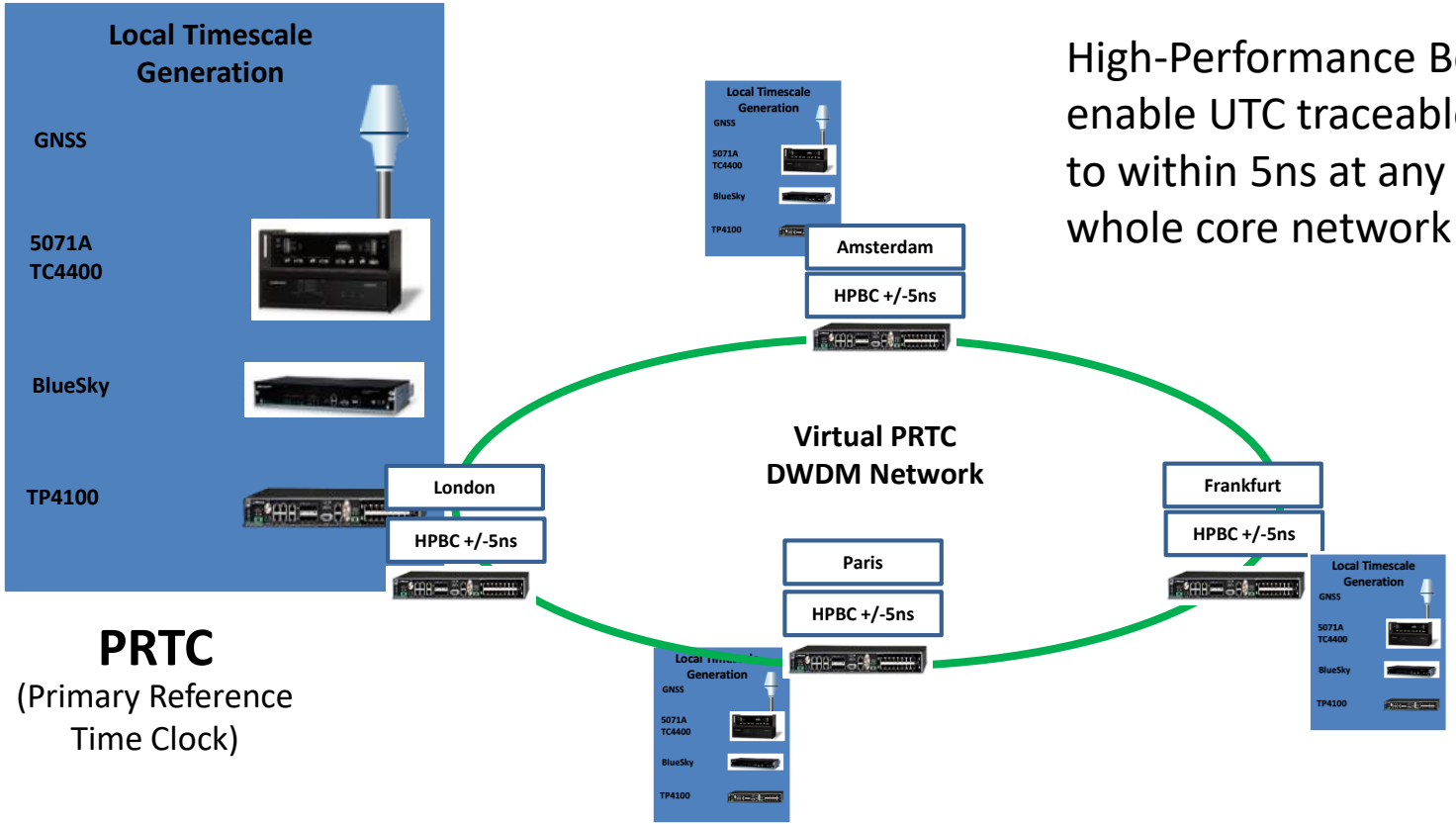


Live Sky
(not secure)

Hardened Output
(secure and resilient
using atomic holdover)

Validated Output

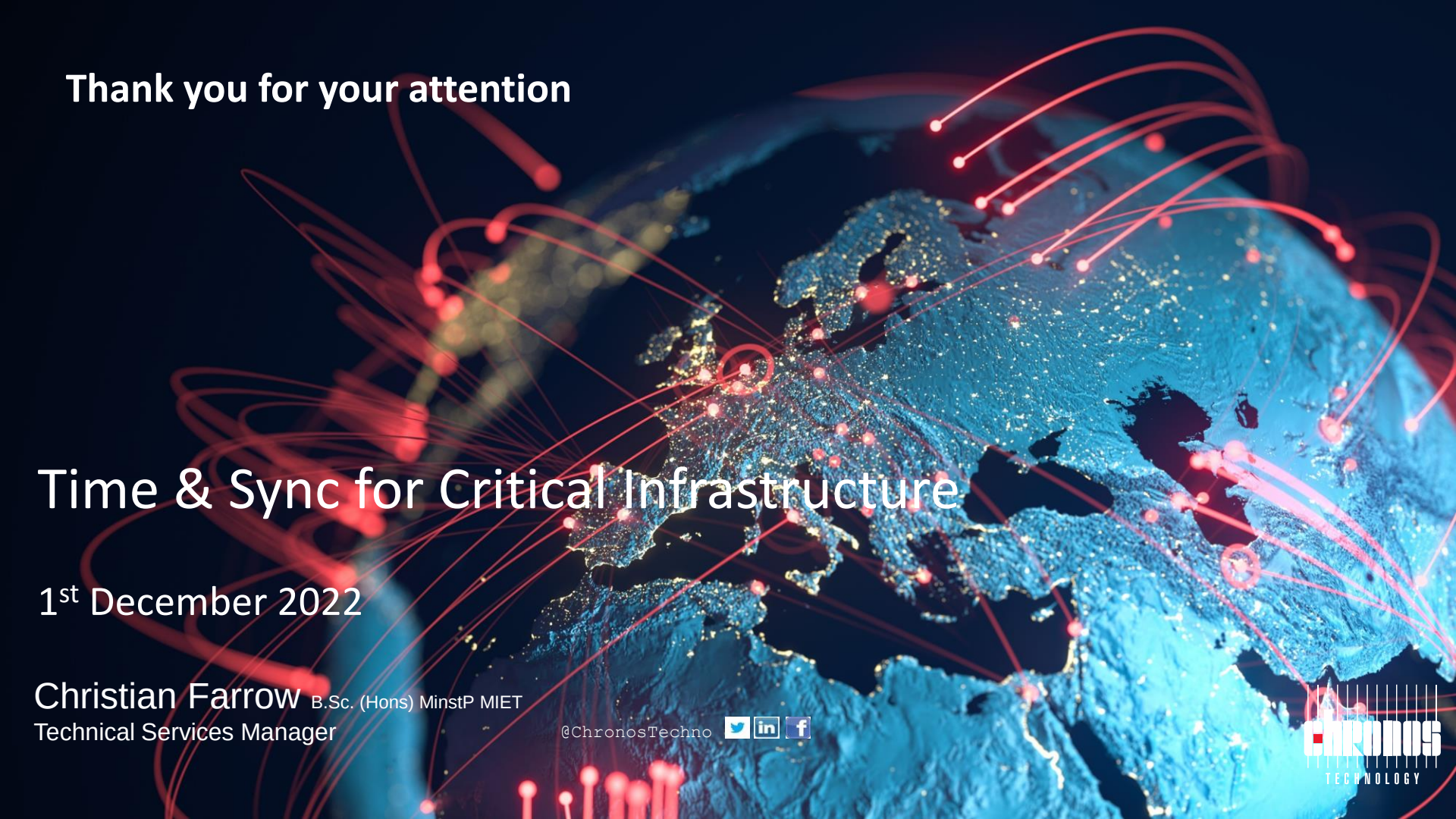
Proposal – The Network as The Clock



High-Performance Boundary Clocks enable UTC traceable time delivery to within 5ns at any point across the whole core network

Summary

- The transition to Smart Grid technology requires careful planning:
  - Time Sync enables new functions & features
  - ...but sources of time need protection from attackers
  - GNSS firewall technology can help
  - Utilise the available Telecom Network resources such as DWDM & HP-BCs to distribute your own time "own your own timescale"!



Thank you for your attention

Time & Sync for Critical Infrastructure

1st December 2022

Christian Farrow B.Sc. (Hons) MinstP MIET
Technical Services Manager

@ChronosTechno

Agenda

Karabo is responsible technical assurance and asset management programs for all the mine's electrical infrastructure. He has experience as protection engineer responsible for the National Transmission grid maintenance and operations.

***Debswana Smart Grid Solution*, Karabo Mmokwa**

DEBSWANA
Mining diamonds, enriching the nation

Asset Management Engineer –for Jwaneng Mine (Debswana).

DEBSWANA

Debswana Diamond Mining Company

SMART GRID

Engineer Karabo Mmokwa Pr. Eng, C.Eng
Engineer Otto Keitumetse Pr Eng.

DEBSWANA

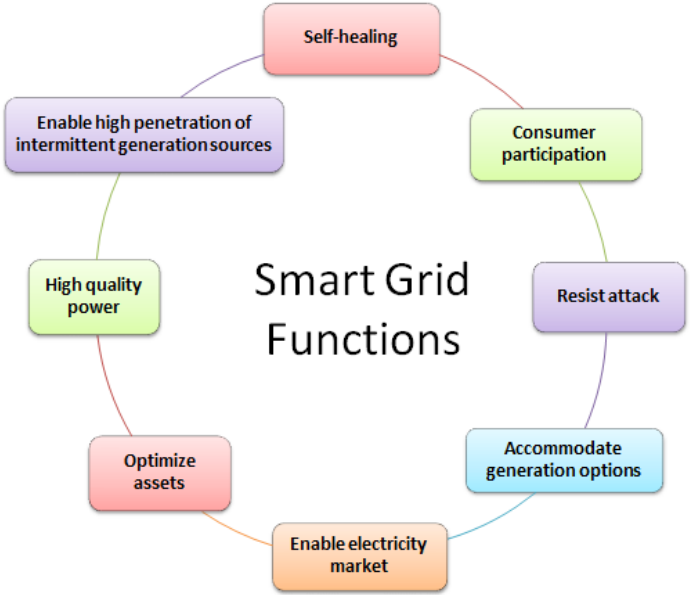
Contents

- What is Smart Grids?
- Driving Factors
- Smart Grid Components-Debswana perspective
- Current Implementation within Debswana
- Benefits
- What's in store for the future?

DEBSWANA

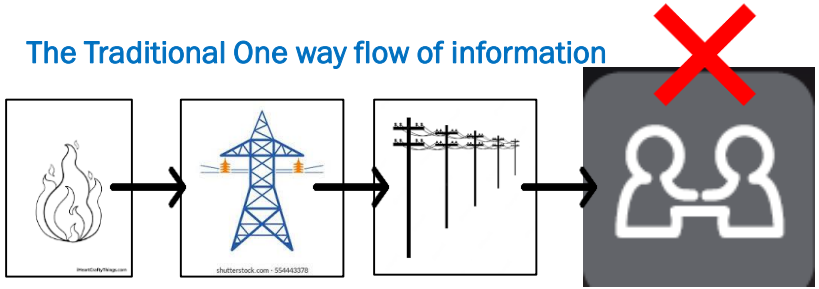
SMART-GRIDS

What is a Smart Grid?



- Distribution Automation
- Conservation Voltage Reduction
- Substation Automation
- Advanced Metering infrastructure(AMI)
- Mobile Workforce automation
- Video Surveillance
- Demand Response
- Integration of Energy Generation sources

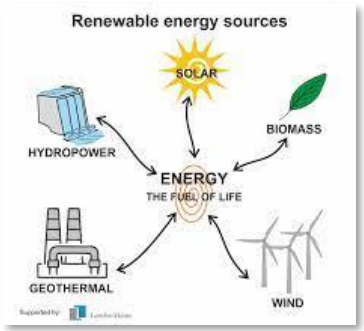
The Traditional One way flow of information

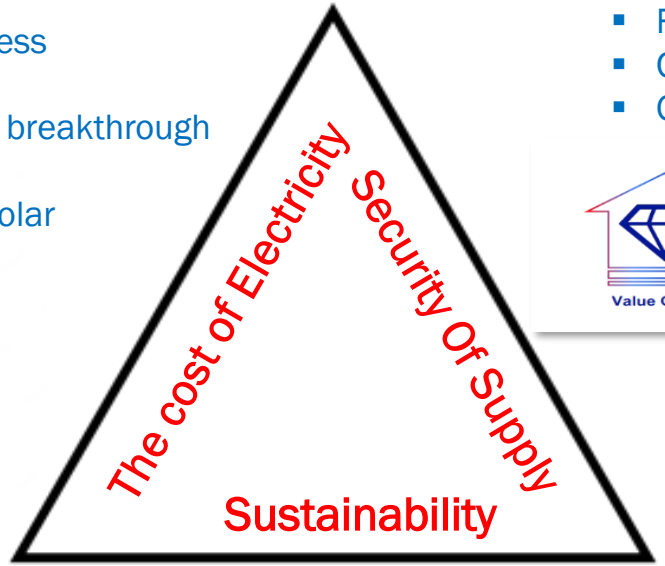


Generation | Transmission | MV Distribution | Energy Consumer

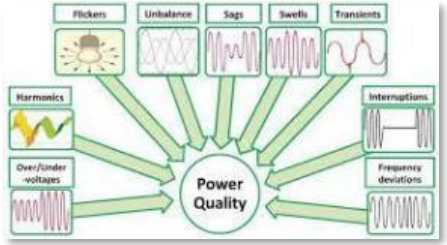
The Smart Grid Driving Factors

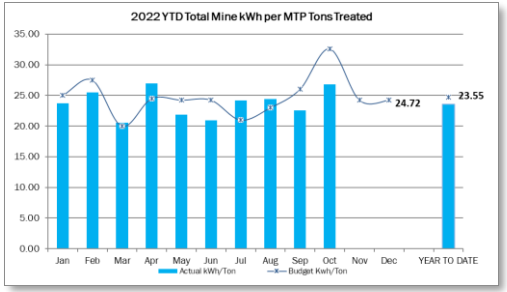
- Innovation for Global competitiveness
- High costs of power
- Shifting Energy demands to match breakthrough targets
- Renewable Projects e.g Roof Top Solar





- Energy availability (depleting resources)
- Reliability and Quality
- Capacity?
- Operational excellence



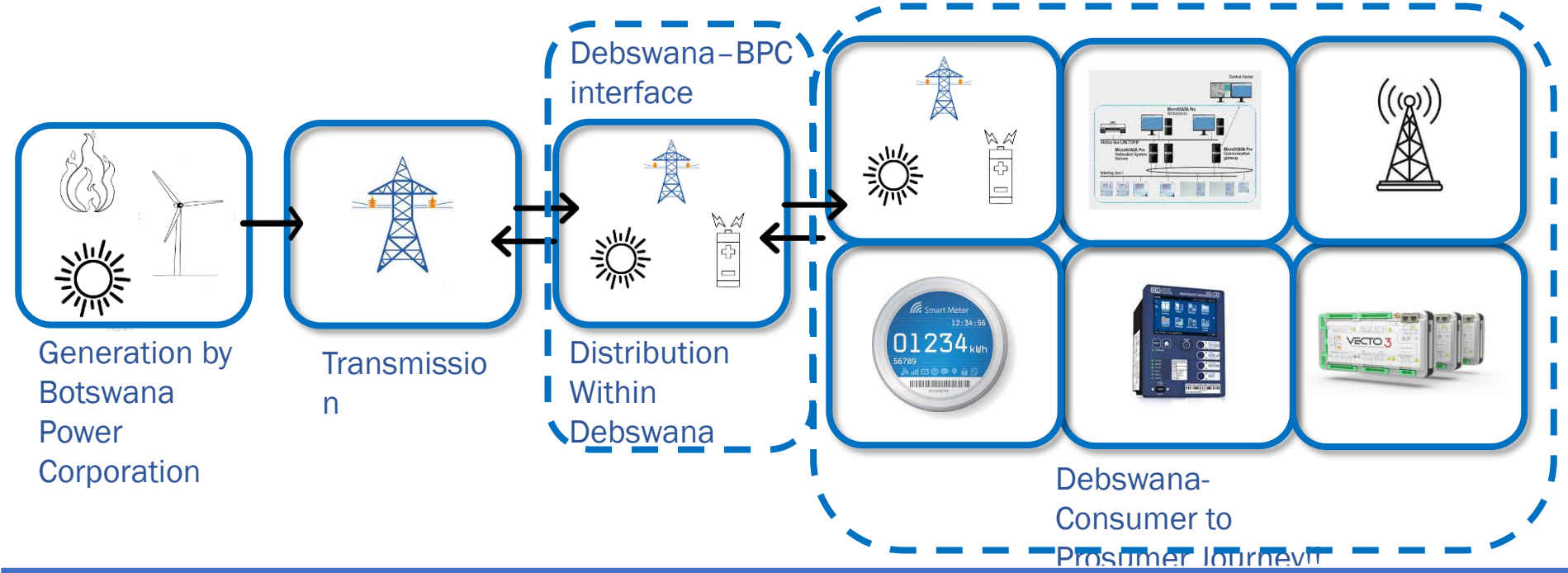


- Safety
- Climate change
- Carbon neutral by 2030
- Sustainable operations is a basic fundament term in **license to operate**


DEBSWANA
Smart Grid Components-
Debswana Perspective

DEBSWANA

The New Energy Land scape Provides Debswana with New Options and Opportunities



Decentralized + Flexible + Connected

DEBSWANA

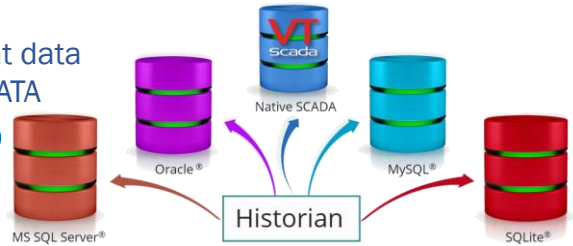
Debswana Smart Metering

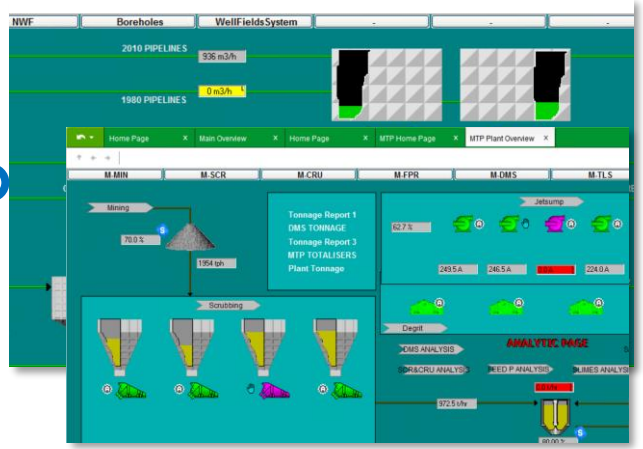
Smart Energy METERS

- Max Demand management
- Consumption
- real time monitoring
- Energy Intelligence
- Fault Detection

Debswana Historian

- Links to critical Plant data
- Feeds Production DATA





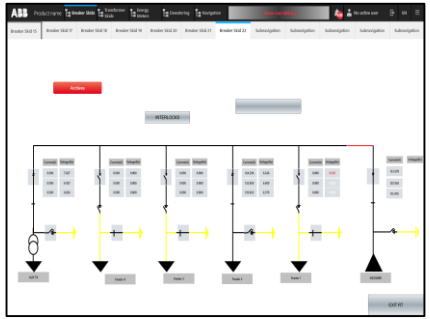
Expert Power software Interface

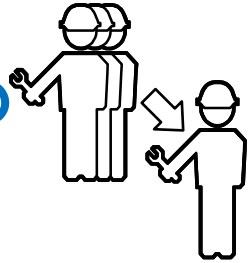
- Billing and Demand response
- Energy management
- Power Quality Visualization
- Consumption and demand trending
- Forecasting for improved performance

DEBSWANA

Debswana Electrical Grid Management - SCADA

- Smart Meter Integration
- IEC 61968
- PQ Metering
- Protection Relays

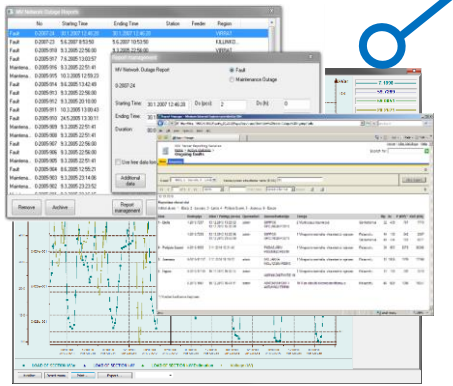




- Crew Team Positioning
- Increased safety
- IEC 61968

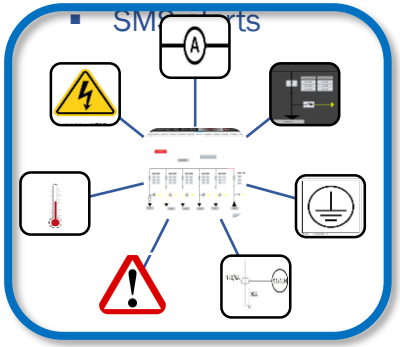
Virtualization

- Remote control
- Load management
- IEC 60870
- IEEE C37.1-2007
- SM[illegible]rts



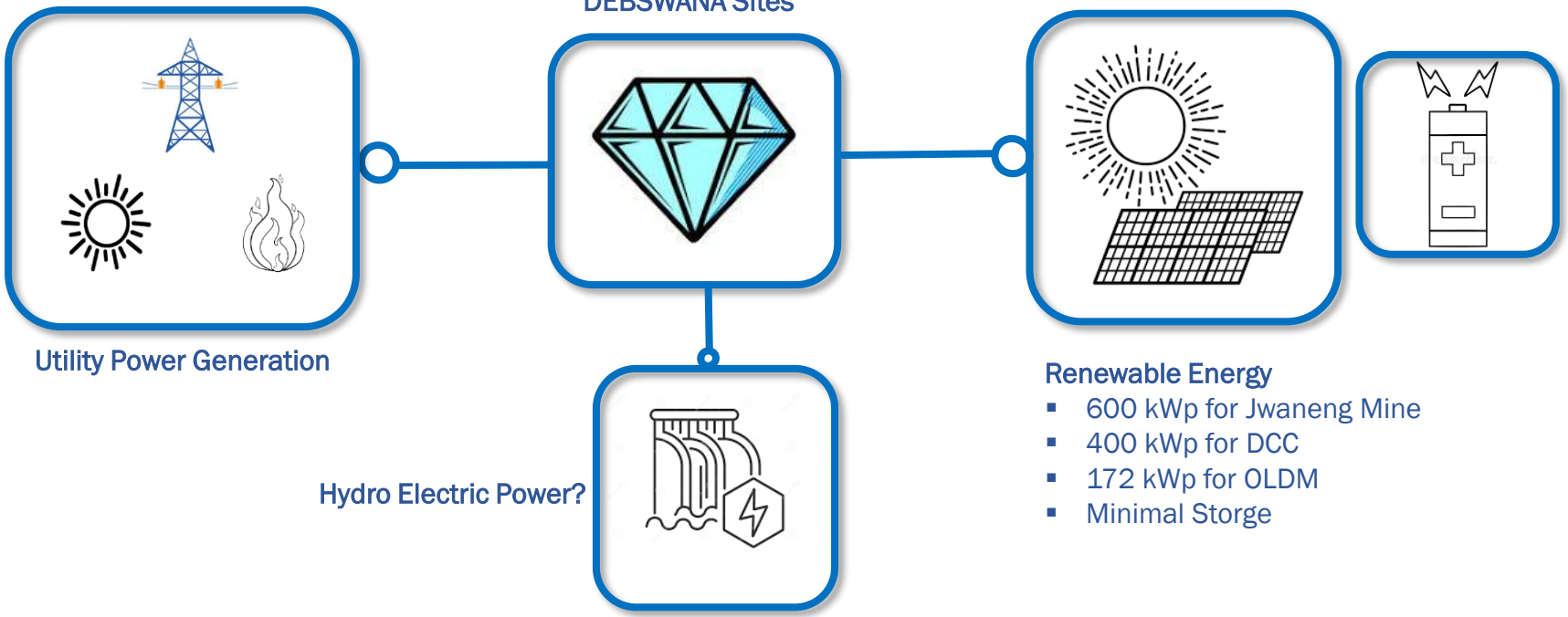
- Real Time Dashboard
- Load Estimation and management
- Short Term load forecasts
- Outage Reporting
- Optima control for energy loss reductions

- Fault Detection information relaying



DEBSWANA

Integrated Energy Sources



DEBSWANA

The Benefits

DEBSWANA

It Makes Business Sense

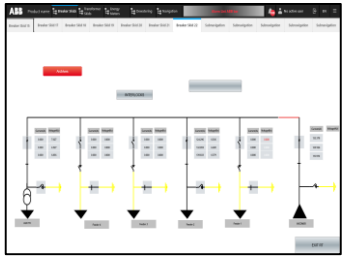
- Improves power distribution reliability by providing centralized visibility and control of intelligent electronic devices (IEDs)
- Lowers costs and improves efficiency by enabling applications such as active Volt/VAR management and conservation voltage reduction
- Decreases expense of retrofitting substations to implement automation
- Increases meter reading accuracy; quickly isolates problems, reducing repair time; enables remote shut off/turn on of utility
- Improves mobile utility workers access to information in the field, increasing efficiency and reducing costs

DEBSWANA

What’s in store for the Future?

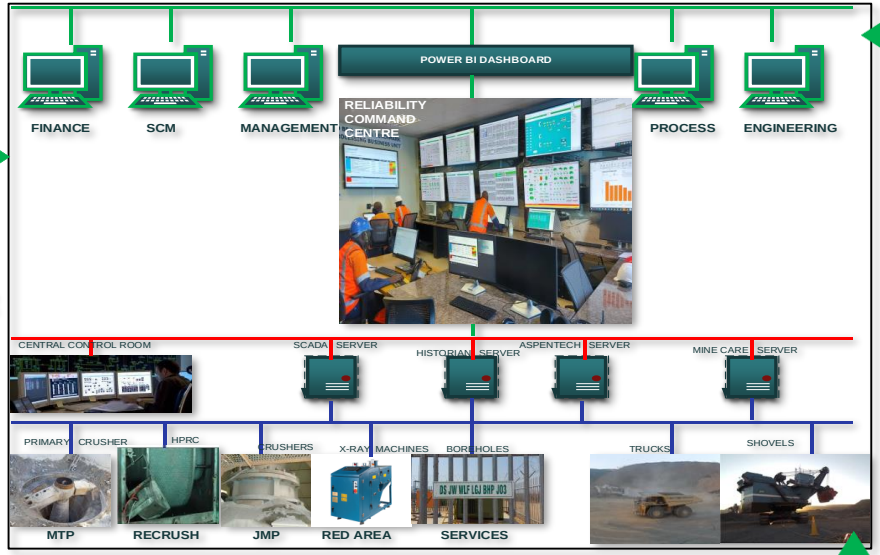
DEBSWANA

Debswana The Command Centers



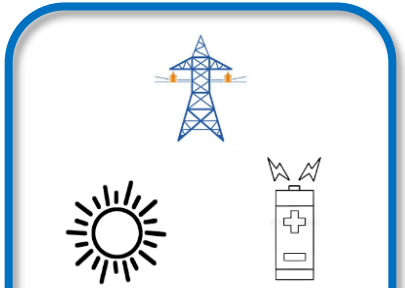
Electrical Network Management

Debswana SMART Metering and Energy Management



Advance Protection systems information

Decentralized Generation



DEBSWANA

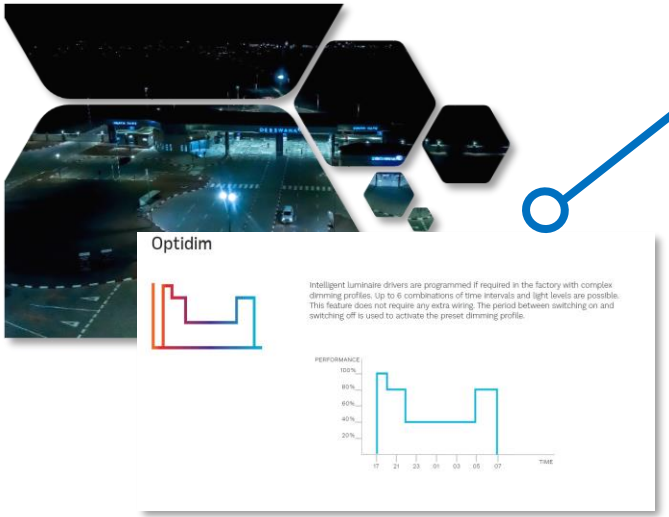
Smart Cities

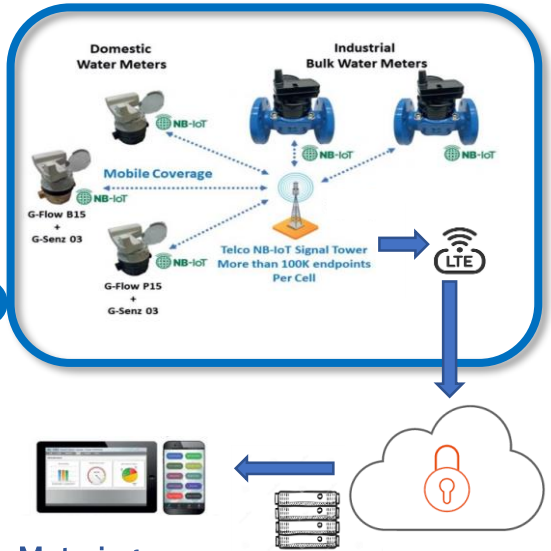
Jwaneng Solar Street Lights

- Optidim Technology

New Orapa West Gate

- Renewable Energy supply
- Solar Street Lights





Jwaneng Smart Water Metering

- Smart Water Meters for Township
- Partnerships with WUC

DEBSWANA

Value levers

- Improved energy security
- Reduced energy cost
- Lower energy emissions

Solution example

Energy Nerve Centre

Data driven insights drive improved Energy Efficiency and Intelligence

Real Time

Real time sensor data to enable the ability to have real time energy information to enable data driven decision making

Historical

Reporting analysis of historic energy data and insight gained from analysis and opportunity

Data Platforms

Integrated well governed data platforms support all processes and all time horizons

Future

Displays past situations and enable chronological navigation, analysis and proactive management of the grid network

Short Interval Control

Enable real-time visualization of the operation

- Controlled emissions
- Circuit management
- Equipment balancing
- Training & coaching
- Utilities Management
- Machine learning
- Real time energy information

Effective maximum demand side management

Payload management

Analyse energy usage

Proactive grid network management

Route optimisation

Active fault finding

Lower fuel spillages

Operator feedback

Reduce energy wastage

IoT sensors for real time data capture

Reduced downtime

More efficient machinery

Timely and informed decisions

On-the-job energy consumption feedback

DEBSWANA

Agenda

Chris is a lead Engineer with 30 year experience in telecoms, networking and cyber security across nuclear, thermal and renewable generation, energy networks, and on and offshore oil and gas.

Lead Engineer- Cyber Security and Telecoms (Offshore) at Scottish Power Renewables

***Zero Trust security in OT*, Chris McGookin,**

Zero Trust in OT

Chris McGookin

Offshore Projects

1st December 2022

SCOTTISHPOWER RENEWABLES

Introduction

SCOTTISHPOWER RENEWABLES

There's a wide range of definitions for "Zero Trust"

- Based on premise there is no such thing as a trusted source.
- Cybersecurity teams need to assume that there are attackers present both inside and outside of their networks, and therefore treat all traffic as suspect.
- No communications should be allowed until each party is properly authenticated and authorized.

CISA

- Zero trust provides a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised. The goal is to prevent unauthorized access to data and services and make access control enforcement as granular as possible. Zero trust presents a shift from a location-centric model to a more data-centric approach for fine-grained security controls between users, systems, data and assets that change over time; for these reasons.

Vendor 1…99

- XXX is the only OT security vendor offering an OT network security solution that integrates with the Zero Trust model for industrial environments. The platform enables users to define access-group segmentation and to enforce Zero Trust capabilities in their OT networks

(Trust no-one!!!)

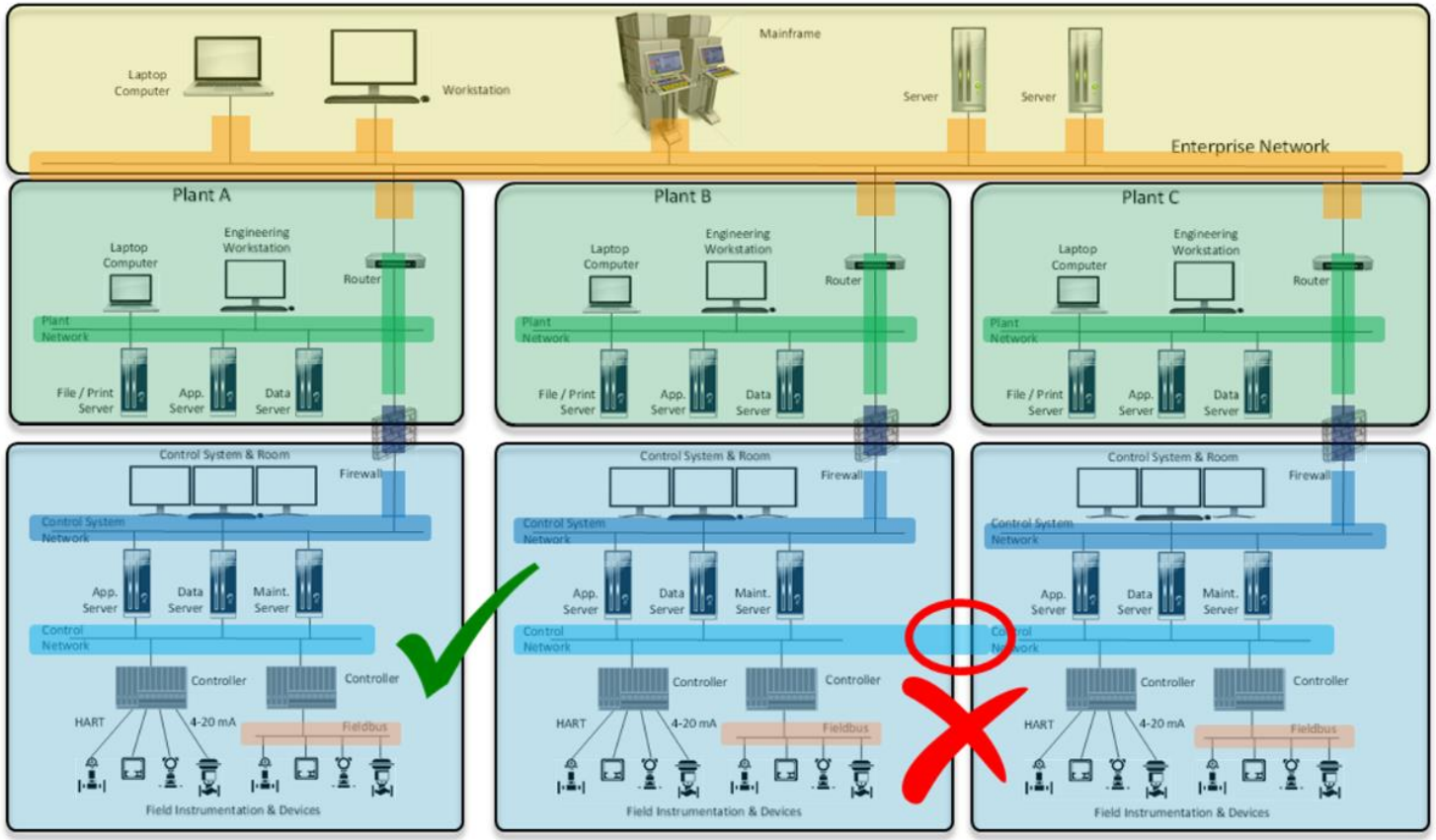
The Problem with Zero Trust in OT

Maybe not the best idea for Cyber Risk Assessment to insist this is a fingerprint scanner…

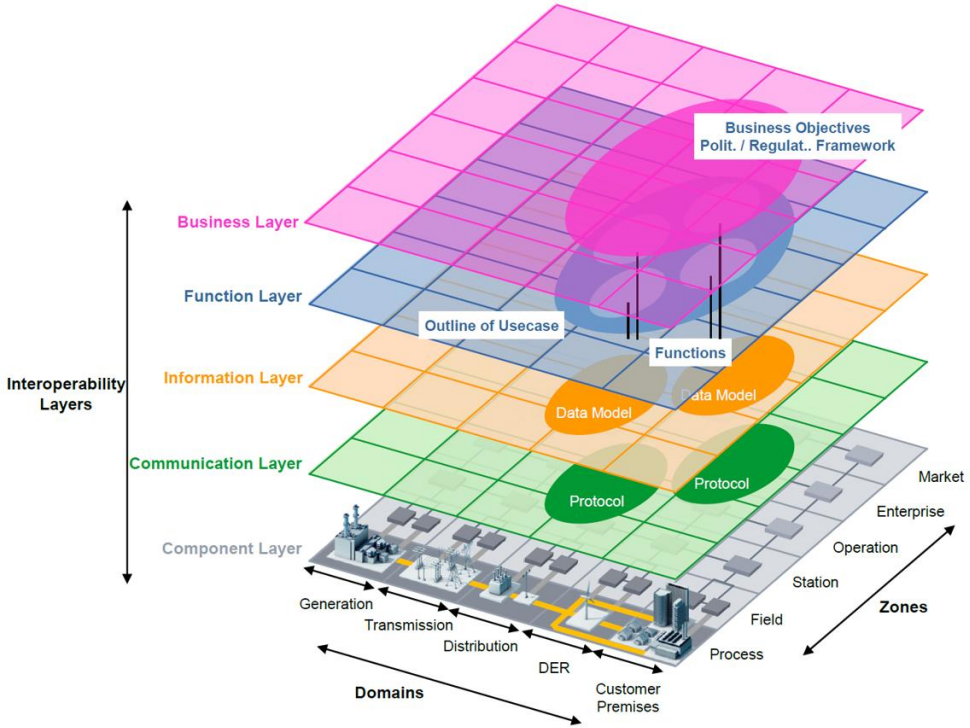
- We don't know if it's a hoax or false alarm- but do we have time or choice to authenticate?
- We trust our instrumentation, people and resources and make decisions based on this
- A break glass may allow minutes to verify. How many milliseconds for protection?
- Could a password/ credential cost life or loss?

SCOTTISHPOWER RENEWABLES

Traditional Segregation of Operational Technology (OT)



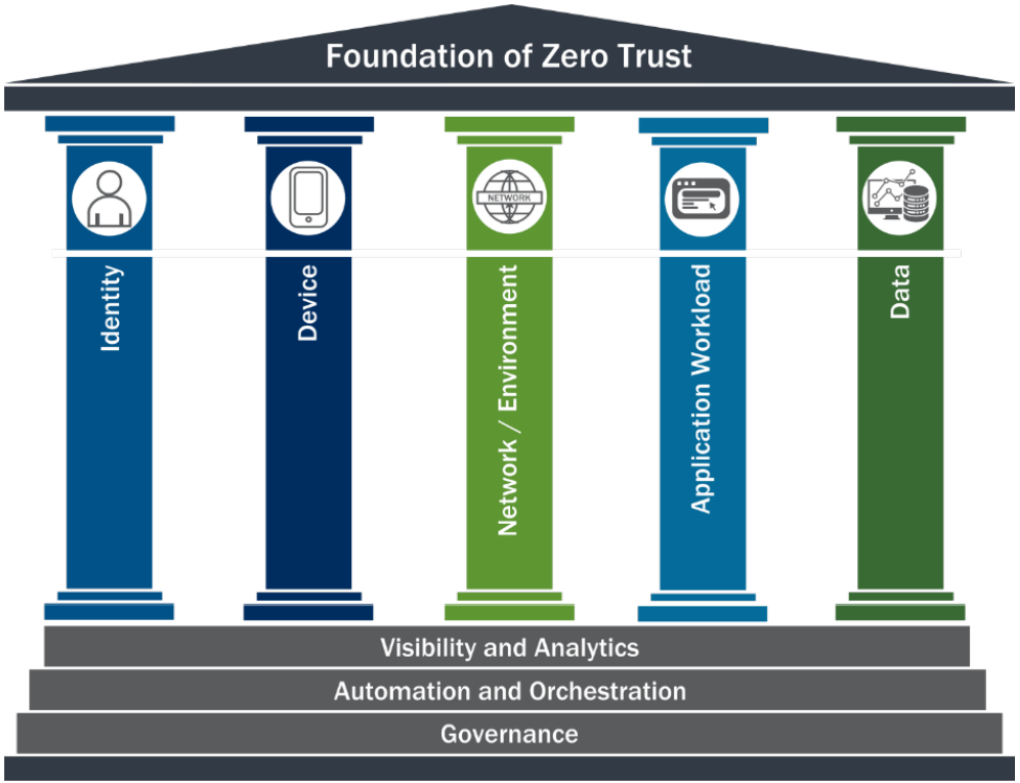
Smart Grid and DER Challenge Traditional Segregation



Smart Grid Architecture Model

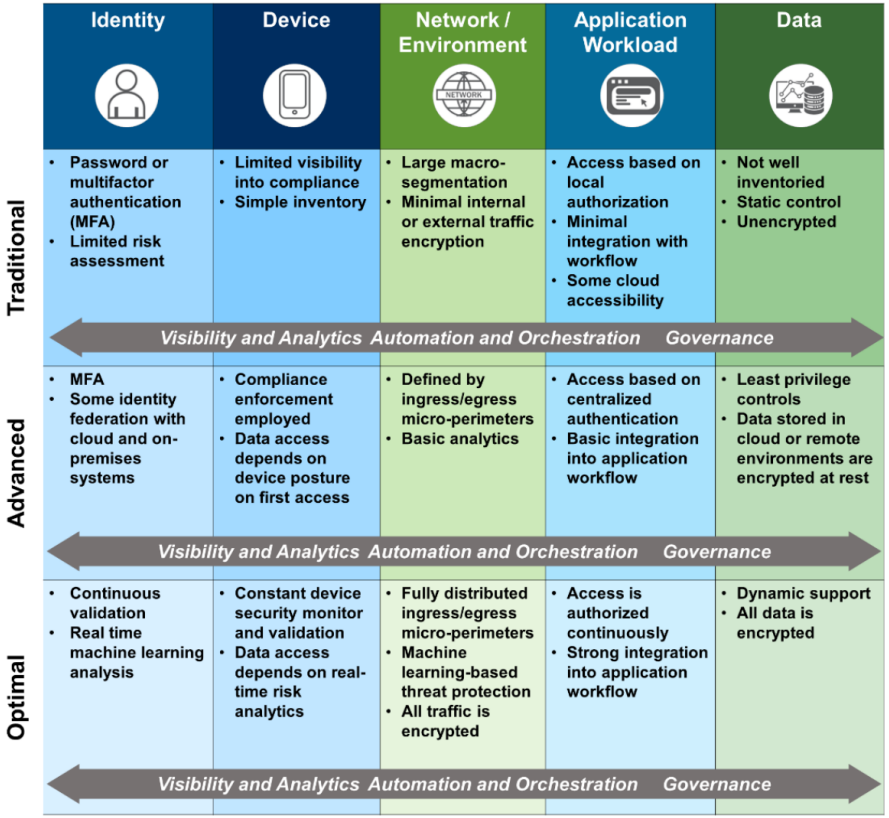
- New Tech- Renewables, Storage, EV, dynamic over/ under rating
- More remote control and automation
- New challenges, scales, lifecycles
- Developing standards and definitions “DER is 10MW, 50MW, >2GW!!”
- Smart Grid is two networks in parallel with new communication flows

The Pillars of Zero Trust



CISA Zero Trust Maturity Model

Zero Trust Maturity Model

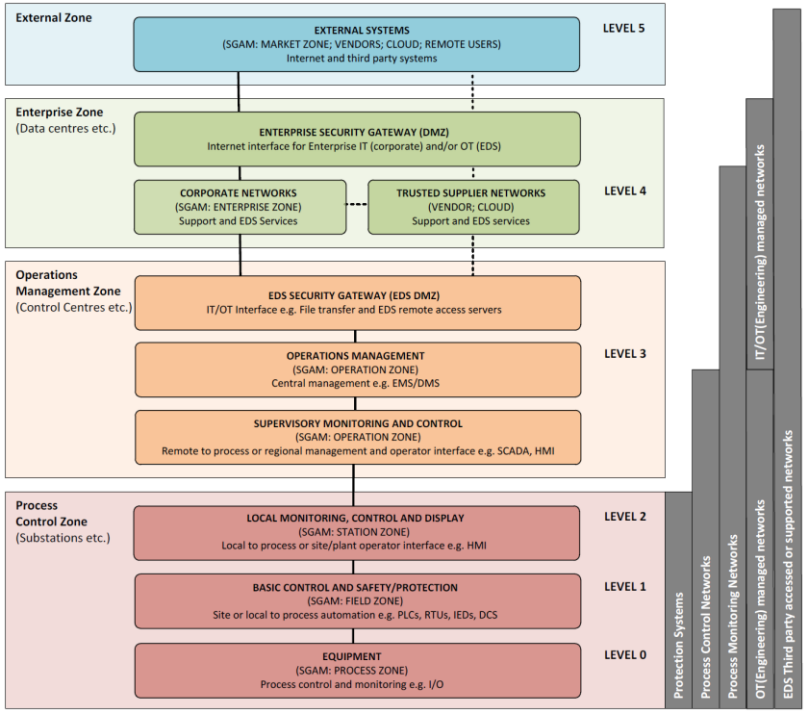


CISA Zero Trust Maturity Model

Support in SCADA and Protection Standards

Standard	Capability
IEC 62351-5	Authentication for IEC 101, 104 and DNP3
IEC 62351-3	Encryption for IEC 62351-5, 61850, ICCP, etc
IEC 62351-6	Authentication for GOOSE and SV
IEC 62351-4	Authentication for MMS.
	The above only protect the SCADA/ Protection Protocol, not management, etc

Summary



BEIS/ ENA Guidelines

- Zero Trust does not honour keep it simple!
- Potential safety conflict- try IEC 61508 SIL assessment on ZTA!
- Upgrade cycles, processing capabilities, bandwidth, vulnerabilities and most importantly availability need factored in Hazop
- Can work well at scale- it's hard to manage security/ firewalls across 500,000 secondary substations or 25 million smart meters
- Hybrids likely

Thank you

www.pndc.co.uk

pndc@strath.ac.uk

@pndc_uk

/company/pndc/