Overcoming the challenges of establishing real-time cyber secure wide area communication between multiple substations

Colin Scoble – Senior Protection Engineer

UK Power Networks
Delivering your electricity

INVESTORS IN PEOPLE™ We invest in people Platinum

NES NATIONAL EQUALITY STANDARD

THE UK'S 25 BEST BIG COMPANIES TO WORK FOR 2021

Agenda

1.	Evaluating the Net Zero situation and challenges we face today
2.	Understanding how the Constellation project will enable secure and flexible network operation with less reliance on the control centre
3.	Implementing effective cybersecurity measures to better protect inter-substation communication
4.	Facilitating smart DSO services through effective local active network management and wide area protection
5.	Mapping out the next steps and how the Constellation architecture can be adopted by the wider IEC 61850 community

UK Power Networks
Delivering your electricity

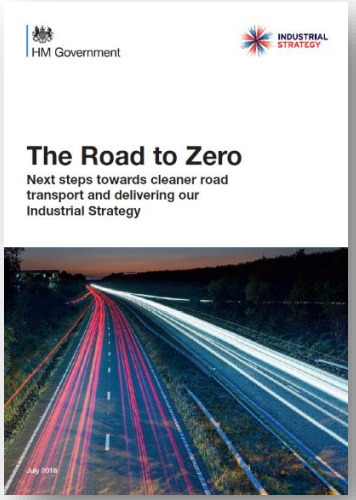
1. Evaluating the Net Zero situation and challenges we face today

UK Power Networks
Delivering your electricity

About UK Power Networks

Measure	Data
End customers	8.3M
Peak demand	16GW
Energy distributed	85TWh
Underground electricity cables	138,000km
Overhead lines	46,000km
Protection relays	45,000
ED1 totex allowance	£6,029M

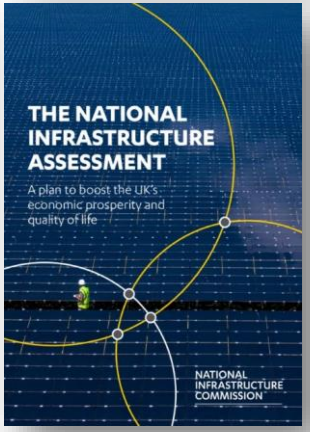
Evaluating the Net Zero challenge we face now



News story

UK becomes first major economy to pass net zero emissions law

New target will require the UK to bring all greenhouse gas emissions to net zero by 2050.



UK Power Networks
Delivering your electricity

Evaluating the Net Zero challenge we face now

Currently deployed technologies

- Smart services rely on Communications back to the control centre central systems
- Transient instabilities create high risk in disconnecting DER's
- Legacy distribution protection methods are not suited for bi-directional power flows
- Significant increase in DG from 26GW now to 65GW in 2050 (GB)
- Smart solutions require significant hardware and Engineering time

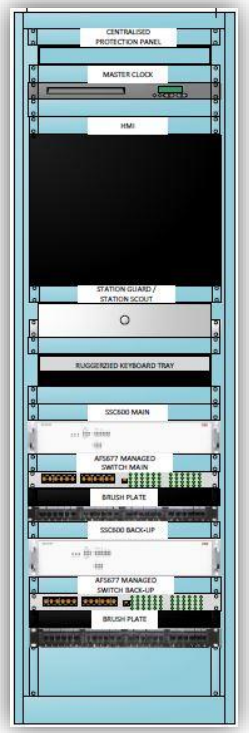
Complications

- Smart services are lost with communications failures: Constraints of 13GW by 2050 (GB)
- Smart DER services are lost due to transient instability events: 14GW in 2050 (GB)
- Static protection settings can restrict the available capacity for DG flexibility services.
- Expensive and slow hardware deployment restricts roll-out of smart solutions

2. Understanding how the Constellation project will enable secure and flexible network operation with less reliance on the control centre

UK Power Networks
Delivering your electricity

Reminder – Unified Protection project (Centralised Protection)



APPROVED

UK Power Networks
Delivering your electricity

Lessons learnt - Unified Protection project

Engineering Lessons learnt

Redundancy creates complex Engineering for the Engineering tools.

Front end specifications and standards need to be validated during pilots.

Engineering control procedures are required for Specifications, Type approvals, FAT's and SAT's.

Not all managed switches are equal…

IEC61850-90-5 and/or C37.118 could add real value to flexible services.

Having backup protection in the bay level IED's can prevent complex redundancy.

Firmware lessons learnt

Firmware upgrades are essential for additional features, bug fixing and security vulnerabilities.

Internal processes need to be in place to deploy firmware upgrades in live systems.

Firmware needs to be validated with the site configurations before being deployed in the live network.

Training lessons learnt

Select technology champions to complete certified training

To develop confidence you need training and experience. Continuity with the technology

Cyber security is a wide stretching field and ever evolving. Continual training is required.

Cyber Security

Virtualisation provides benefits for Cyber security strategies.

Multiple IDS systems trialled.

Data transfer requirements to centralised systems are considerable against conventional systems.

Using IEC 62351 to guide your Cyber strategy sets you on the right path.

IED Vendors need to work faster to implement Cyber features such as SNMP V3…

UK Power Networks
Delivering your electricity

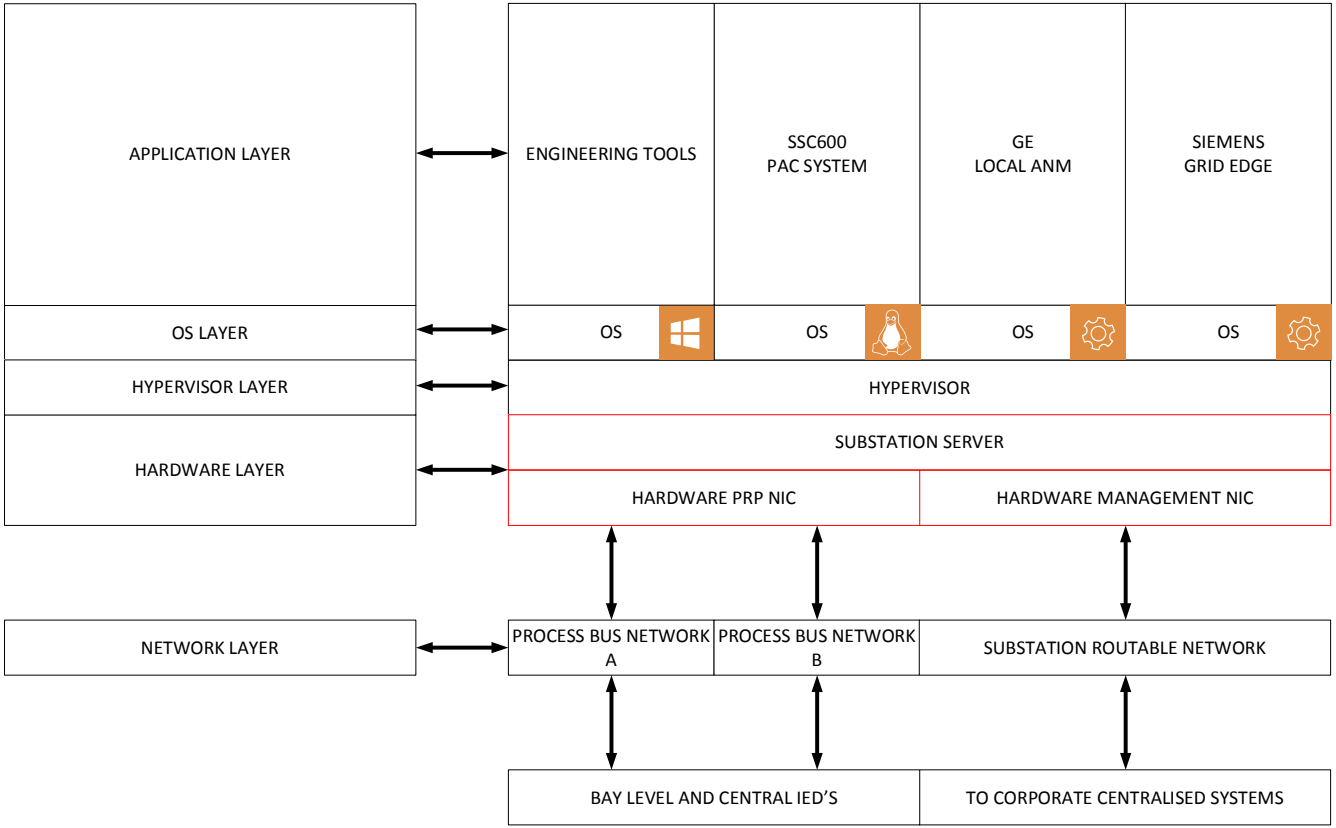
Our motivation for Constellation…

We have a Substation Server…

Could we run this application on the Substation Server?

UK Power Networks
Delivering your electricity

Our motivation for Constellation…



UK Power Networks
Delivering your electricity

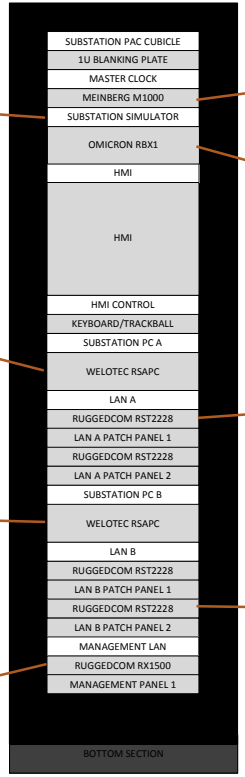
Constellation - Design

Substation IEC61850 Test System

Main Substation Server

Backup Substation Server

Substation Routable network



IEEE1588 Clock

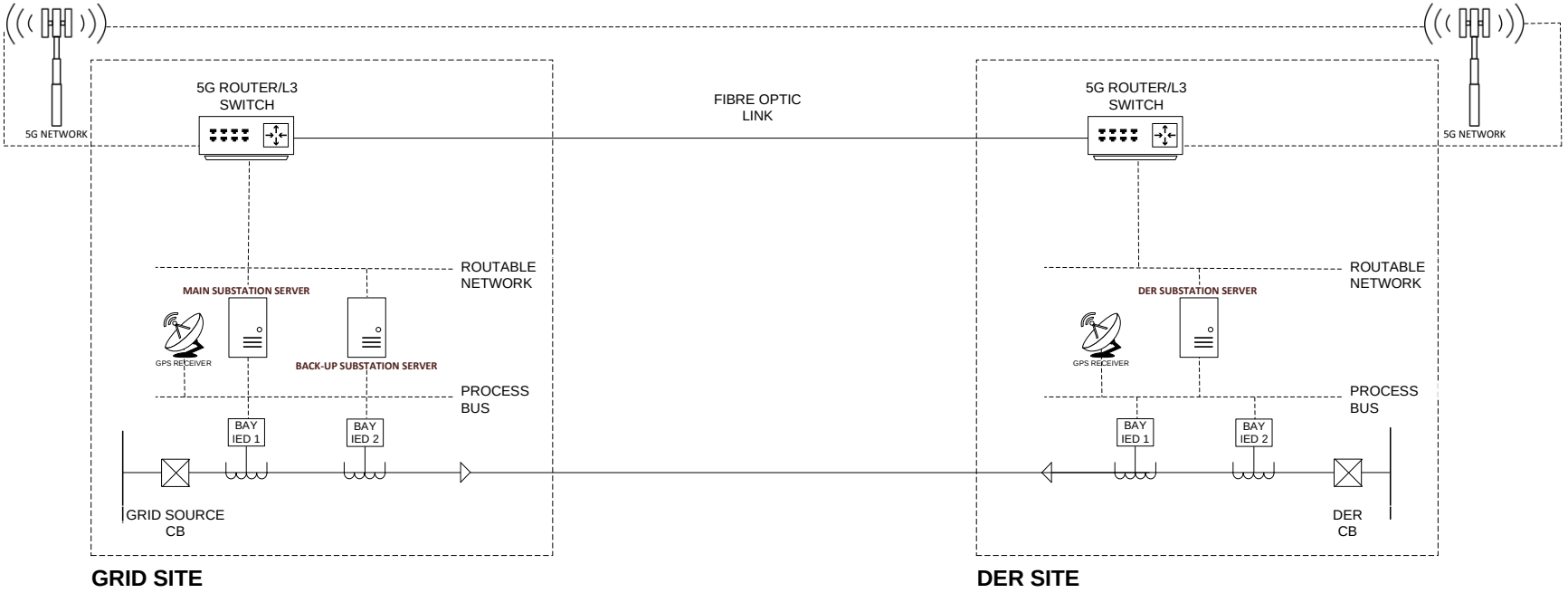
IDS

Substation PRP Network A

Substation PRP Network B

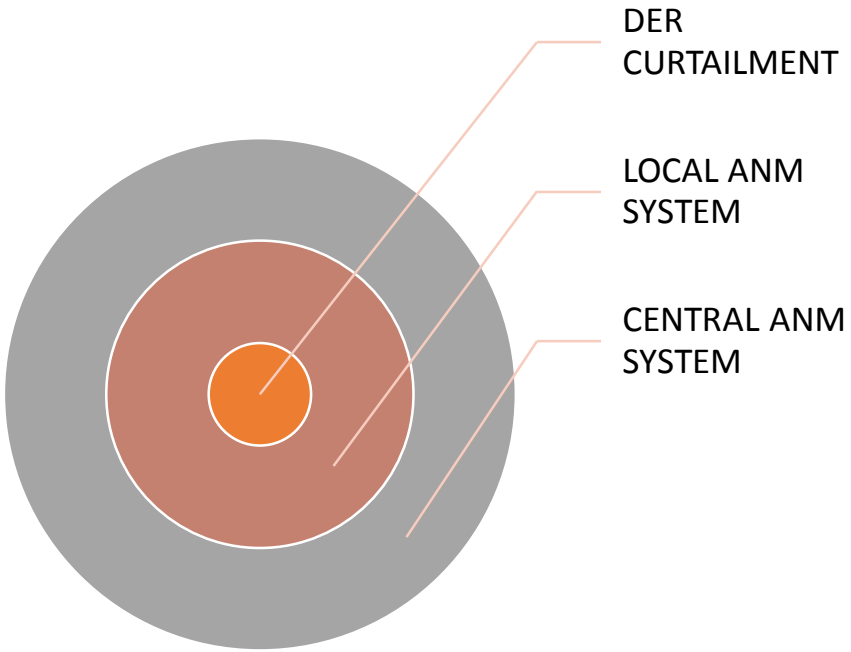
UK Power Networks
Delivering your electricity

Simplified site to site communications



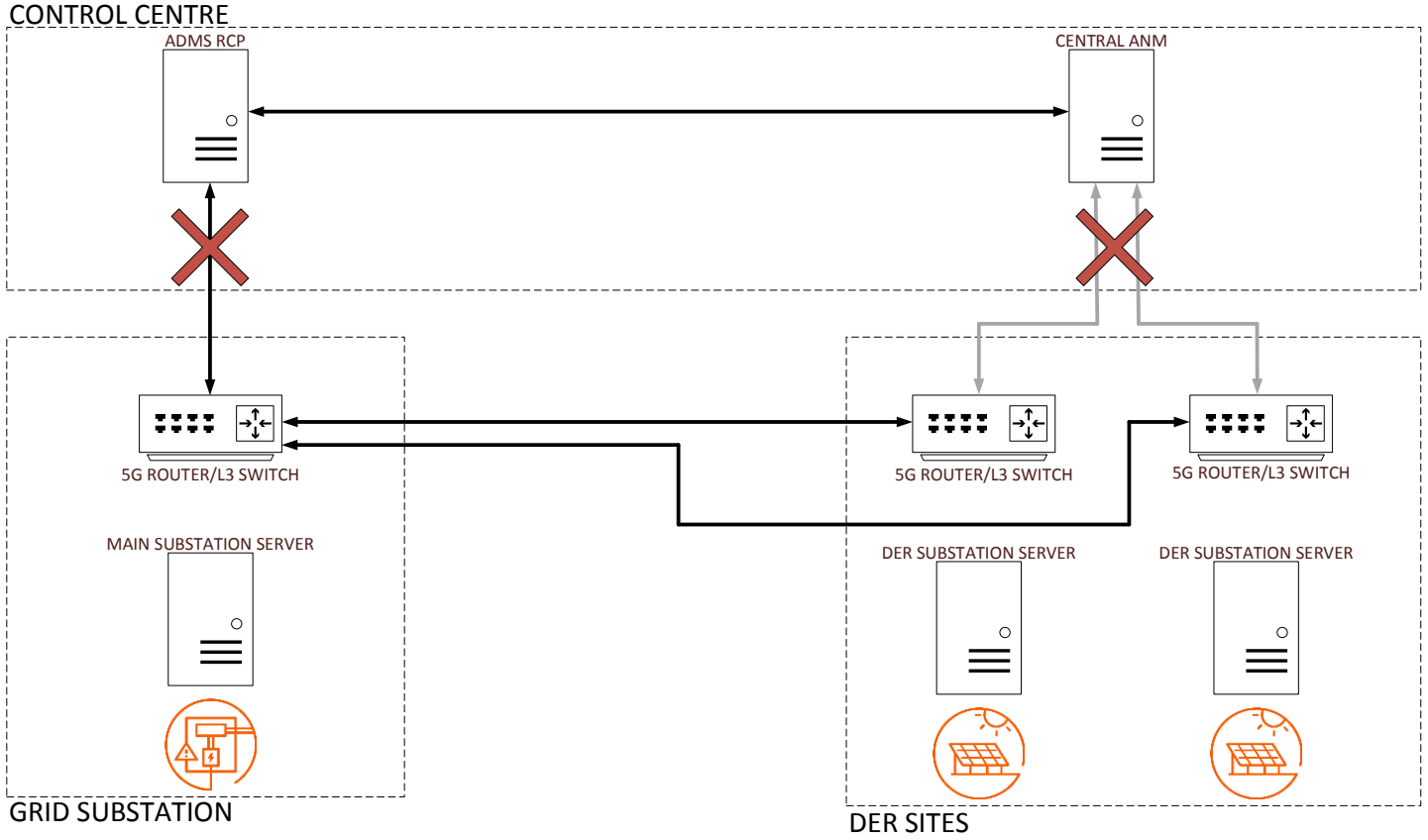
UK Power Networks
Delivering your electricity

Onion layer approach to PAC systems – Local ANM



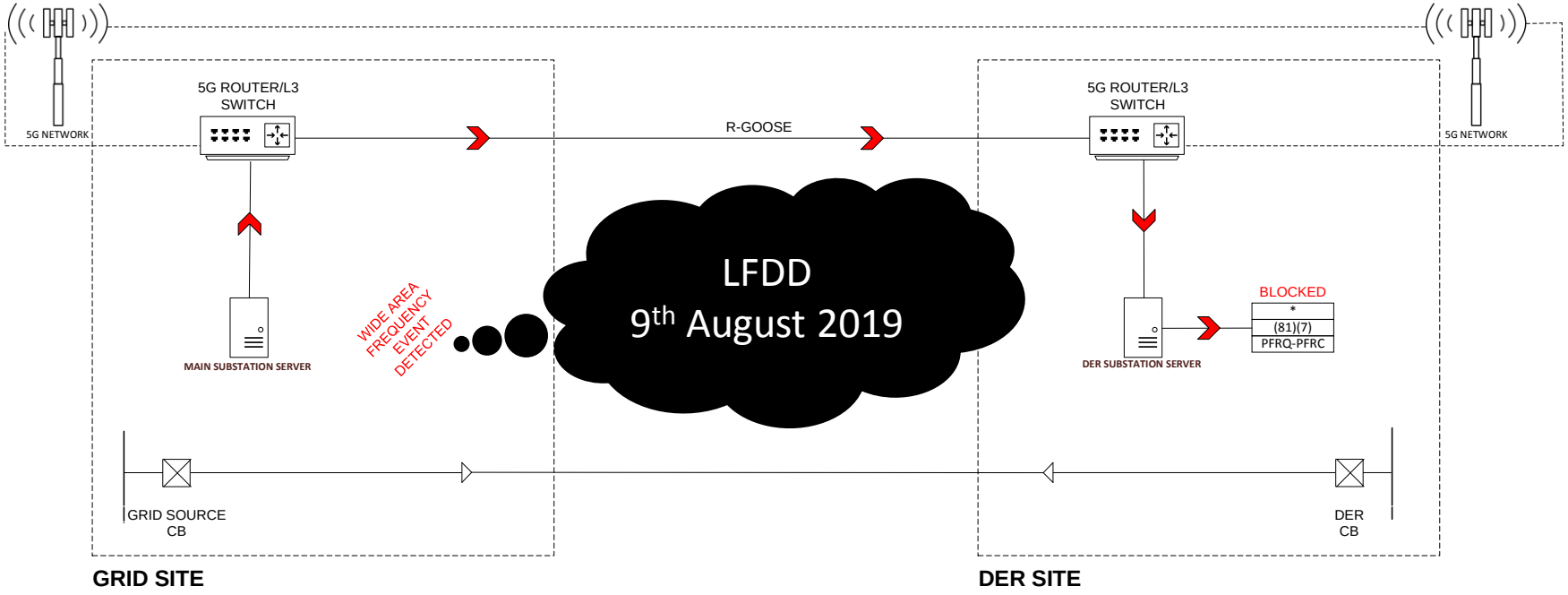
UK Power Networks
Delivering your electricity

Local active network management



UK Power Networks
Delivering your electricity

Wide area protection applications



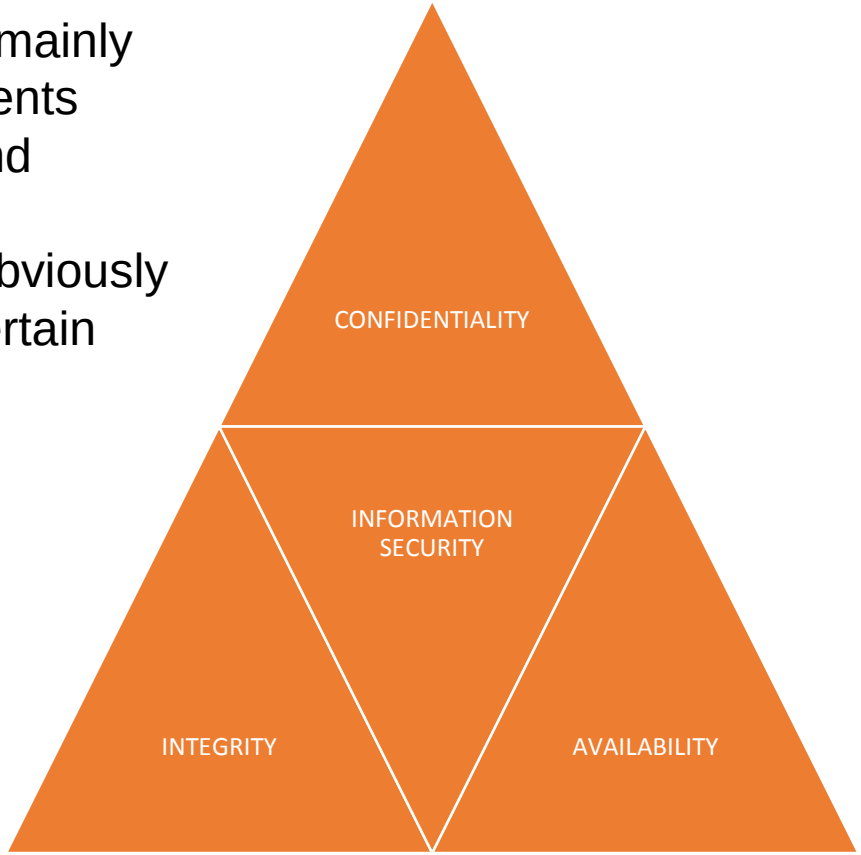
UK Power Networks
Delivering your electricity

3. Implementing effective cybersecurity measures to better protect inter-substation communication

UK Power Networks
Delivering your electricity

CIA TRIAD

- O/T Networks are mainly focussing investments around Integrity and availability.
- Confidentiality is obviously still important in certain circumstances



IEC 62351

IEC 62351 PART 3	• TCP/IP PROFILES
IEC 62351 PART 4	• TLS Encryption for Profiles including MMS and derivatives (hardcopy version only)
IEC 62351 PART 5	• Profiles including IEC 60870-5 and derivatives (e.g. DNP3 derivative)
IEC 62351 PART 6	• Security for IEC 61850 profiles (IEC 61850-8-1(MMS), IEC 61850-8-2, IEC 61850-9-2(SMV) and IEC 61850-6)
IEC 62351 PART 8	• Role-based access control
IEC 62351 PART 9	• Key Management

CYBER SECURITY RISK ASSESMENT

#	Risks*	Severity	Likelihood
1.	Part of the 5G hardware is on a logically shared physical infrastructure		
2.	5G network operator power supply resilience at the masts		
3.	GPS jamming/spoofing will affect GPS clocks and time stamp of data		
4.	Substation server unauthorised access		
5.	Asset firmware vulnerabilities		
6.	Cyber Squirrels (Cybersquirrels1.com)		
7	Security of data		
8	Engineering configuration corruptions (accidental error)		

** This is not an exhaustive list and it contains a draft risk assessment which will be validated throughout the project*

CYBER SECURITY COUNTER MEASURES

DESCRIPTION	Confidentiality	Integrity	Availability	Risk Management
Secure time based password control	√	√		4,7,8
IDS and Audit logging (Syslog, SIEM)	√	√	√	4
Virtual Private Network (IPSec)	√	√		1,4,7
Role based access control & session recording	√	√		4,7,8
IEC 62351 Security for DNP3 (DER Cont.)	√	√		4,7
Communication path resilience			√	2
Network and System Management			√	4,5
Hypervisor VM image back up		√	√	7,8
Asset visibility & firmware management (UKPN SCC)			√	4,5
FAT/SAT Testing pre firmware roll out			√	5,8
GPS spoof detection (Alt. Time source x 3)			√	3
VLAN and Subnet Segregation of traffic			√	4,7
Vermin proof specifications for communication paths			√	6

CYBER SECURITY RISK ASSESMENT – CONTROL MEASURES IN PLACE

#	Risks*	Severity	Likelihood
1.	Part of the 5G hardware is on a logically shared physical infrastructure		
2.	5G network operator power supply resilience at the masts		
3.	GPS jamming/spoofing will affect GPS clocks and time stamp of data		
4.	Substation server unauthorised access		
5.	Asset visibility, vulnerability register and Firmware management		
6.	Cyber Squirrels (Cybersquirrels1.com)		
7	Security of data		
8	Engineering configuration corruptions (accidental error)		

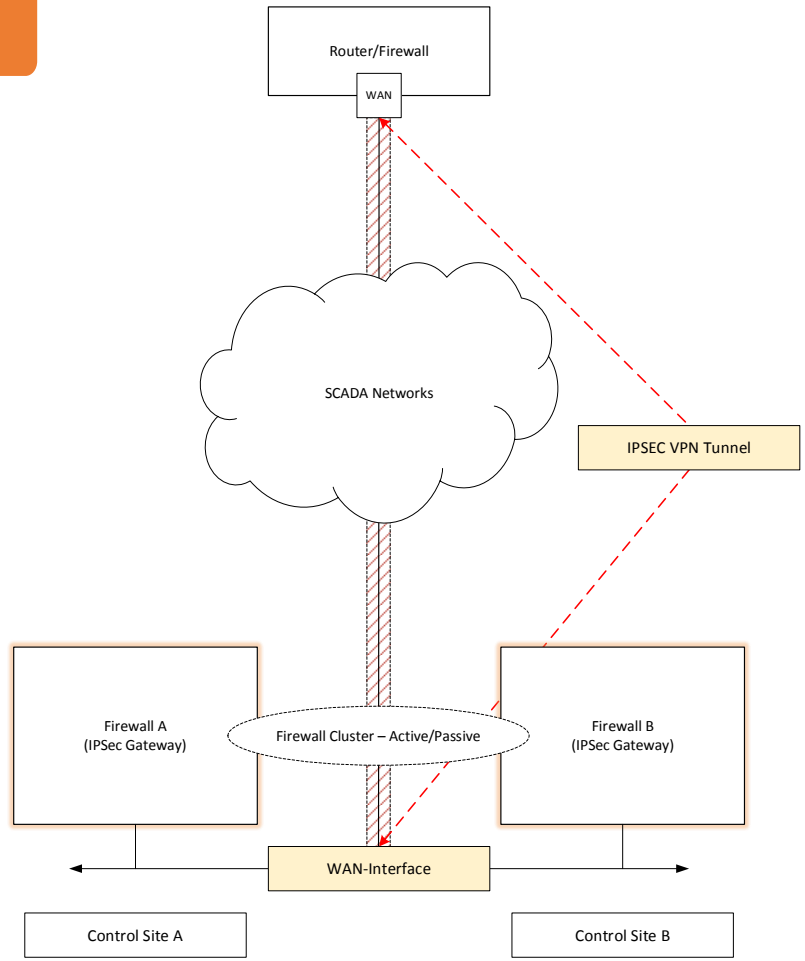
** This is not an exhaustive list and it contains a draft risk assessment which will be validated throughout the project*

IPSEC TUNNELS

An IPSec Site to Site VPN Tunnel will be used to create the secure communications path between the control centre and the substation.

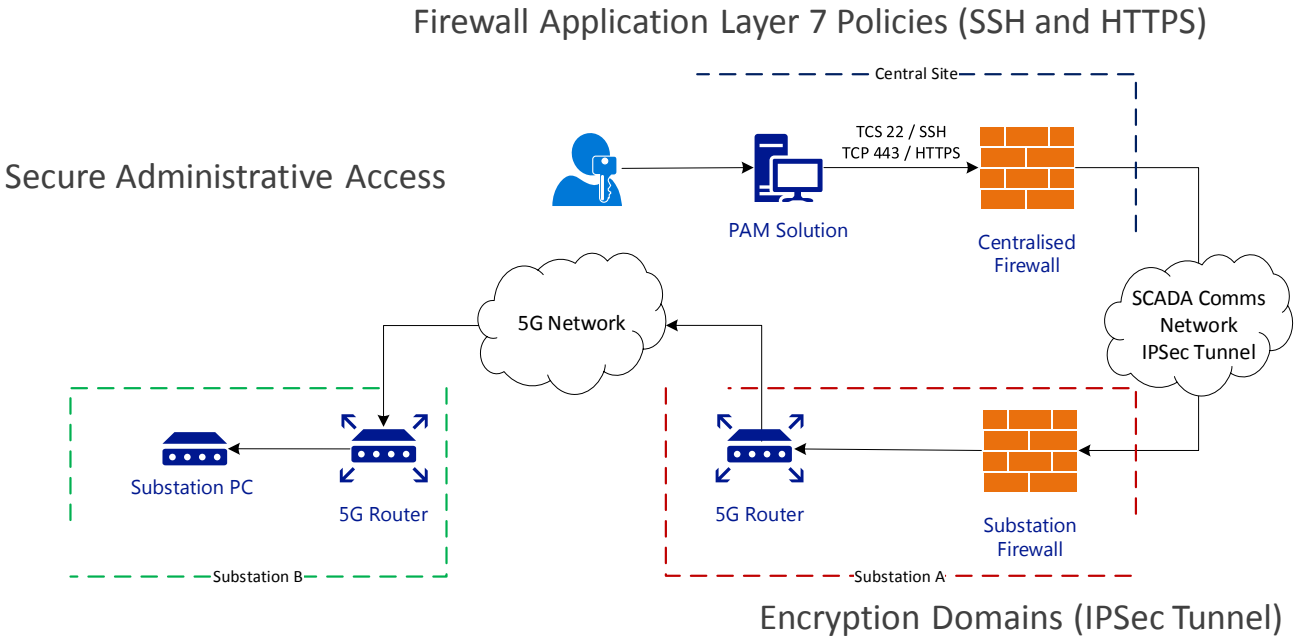
The benefit of using a site to site IPSec VPN Tunnel between the control centre and the substation can be described as;

- IPSec operates below the transport layer (TCP/UDP) so is transparent to the applications
- End to End fully encrypted IP domains
- Fully routable network at the substation (removing the need for PAT – Port Address Translation)
- Network Control – Control over the IPSec Tunnels (enable/disable)



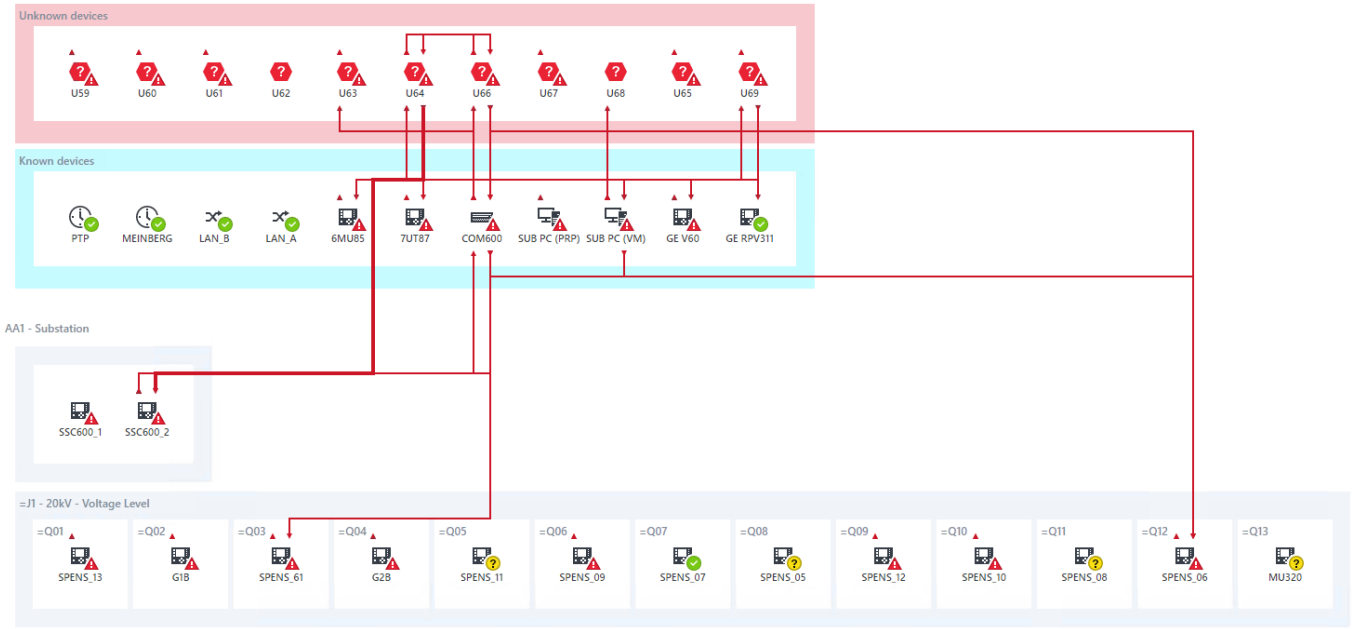
USING PAM WITH SECURE PROTOCOLS

- Use of Individually Identifiable Users with 2FA Access
- Fully Auditable with Session Recording for Restricted & Controlled Access
- Password or Certificate Managed Access



IDS AND AUDIT LOGGING (SYSLOG/SIEM)

- Identifying unknown devices on the substation network.
- Understanding normal traffic behaviour from devices based on type.
- Interpretation of SCD files to automate norm for the substation.
- Reviewing and whitelisting of protocol traffic.



NETWORK SEGREGATION

Network segmentation involves splitting the larger network into smaller network segments. It may be completed by using VLANs and Smaller Broadcast Domains for Layer 3 (IP)

In a substation environment, traffic could be separated in to VLANs in the following way:

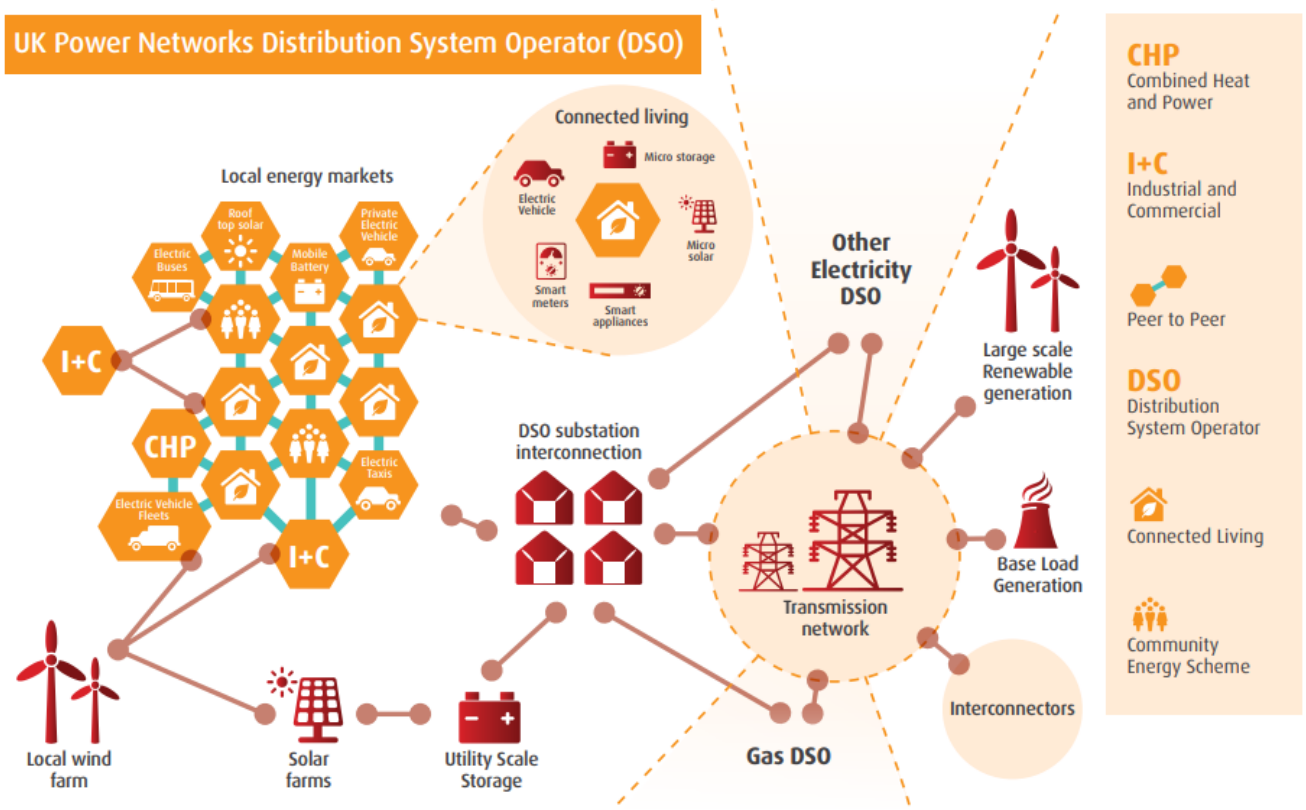
- Management Traffic
- GOOSE Traffic
- Sample Values Traffic
- MMS Traffic

- VLANs divide Layer 2 broadcast domains and serves as a first security barrier by inhibiting potential denial of service attacks to all devices, since access to the VLAN is entirely governed by the switch.
- For devices to communicate between each other over different VLANs a Layer 3 router is required.

4. Facilitating smart DSO services through effective local active network management and wide area protection

UK Power Networks
Delivering your electricity

Facilitating smart DSO services through local network operation



Keys to maximising smart services:

- Digitalised substations
- Inter-substation communication
- Security – physical and cyber

Forecasted DSO benefits

Local ANM:

- **Financial** – reduce over-procurement of flexibility services
- **Financial** – deployment of software instead of hardware
- **Carbon** – reduced curtailment of low carbon generation

GB Benefits	£	CO_2
2030	57.1m	0.2m tCO_2
2050	416.5m	1.9m tCO_2

Wide Area Protection:

- **Financial** – reduce over-procurement of flexibility services
- **Financial** – deployment of software instead of hardware
- **Financial** – cost effective site-to-site communication
- **Carbon** – reduced curtailment of low carbon generation

GB Benefits	£	CO_2
2030	74.8m	0.9m tCO_2
2050	347.7m	9.6m tCO_2

Other DSO benefits:

- Resilience for Electricity System Operator (ESO) services (e.g. FFR)
- Local dispatch of DSO services
- Community energy services

5. Mapping out the next steps and how the Constellation architecture can be adopted by the wider IEC 61850 community

UK Power Networks
Delivering your electricity

Project timeline

Nov 2020

Funding award

OFGEM Awarded funding for the project

2021

Design & Procure

Design Phase and procurement of systems

2022

Develop & PNDC trials

Testing phase, analysis of performance and network installation

2023

Passive Network trials

System installed on network and running passively

2024

Active network trials

System actively controlling the network

2025

BAU

Write up the results and iterate system for business as usual

UK Power Networks
Delivering your electricity

Our Partners

Without our partners this project would not have been possible!

NIC - Constellation

colin.scoble@ukpowernetworks.co.uk

Boris.Yazadzhiyan@ukpowernetworks.co.uk

UK Power Networks
Delivering your electricity

Thank you!

UK Power Networks
Delivering your electricity