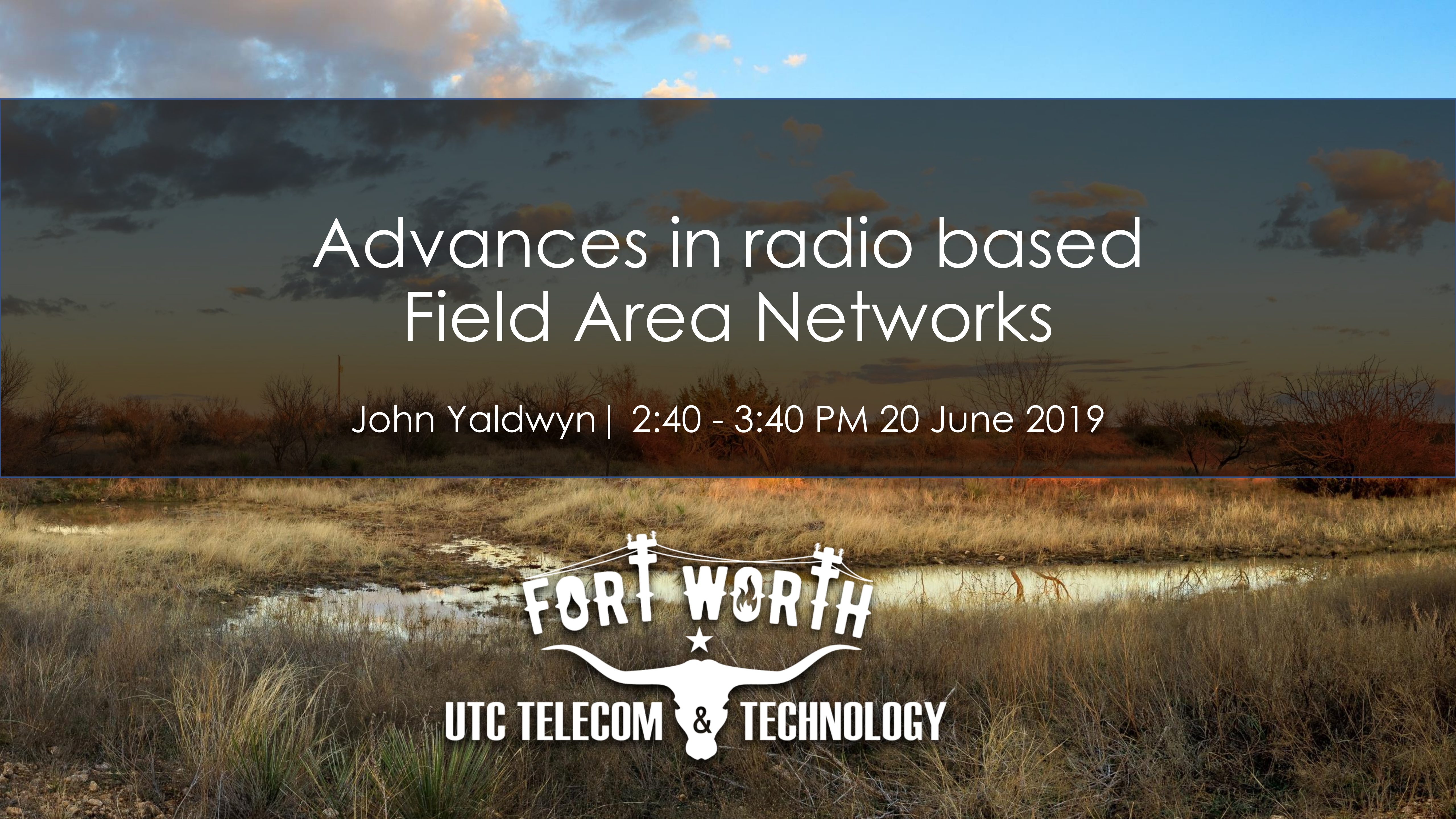


Advances in radio based Field Area Networks

John Yaldwyn| 2:40 - 3:40 PM 20 June 2019

FORT WORTH

UTC TELECOM & TECHNOLOGY

FAN deployments multi-band multi-application

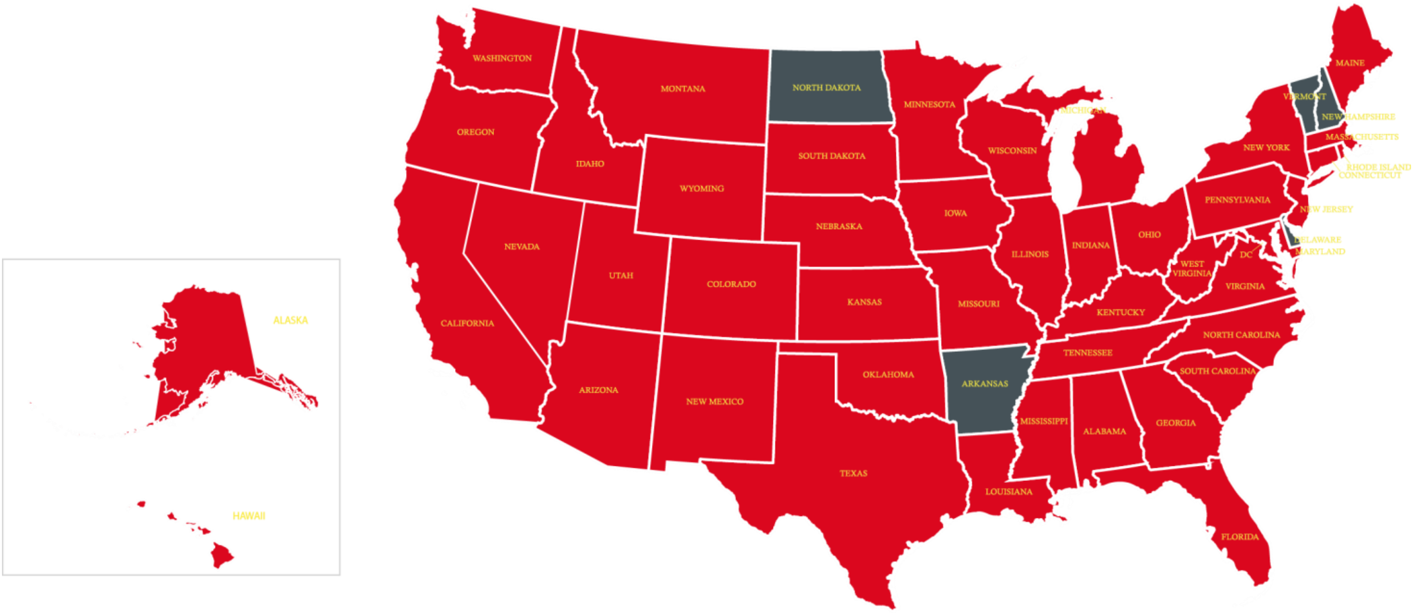
Spectrum – licensed VHF to 900 MHz and unlicensed 902-928 MHz

- Multi-band FAN

DA needs and FAN capacity – radio based FAN and LTE

- Multi-application FAN
- Antennas and lightning protection

Serial, IP and security features



UTC Utilities Technology Council™

FORT WORTH UTC TELECOM & TECHNOLOGY

FAN technology toolbox for the smart grid and other M2M / IoT

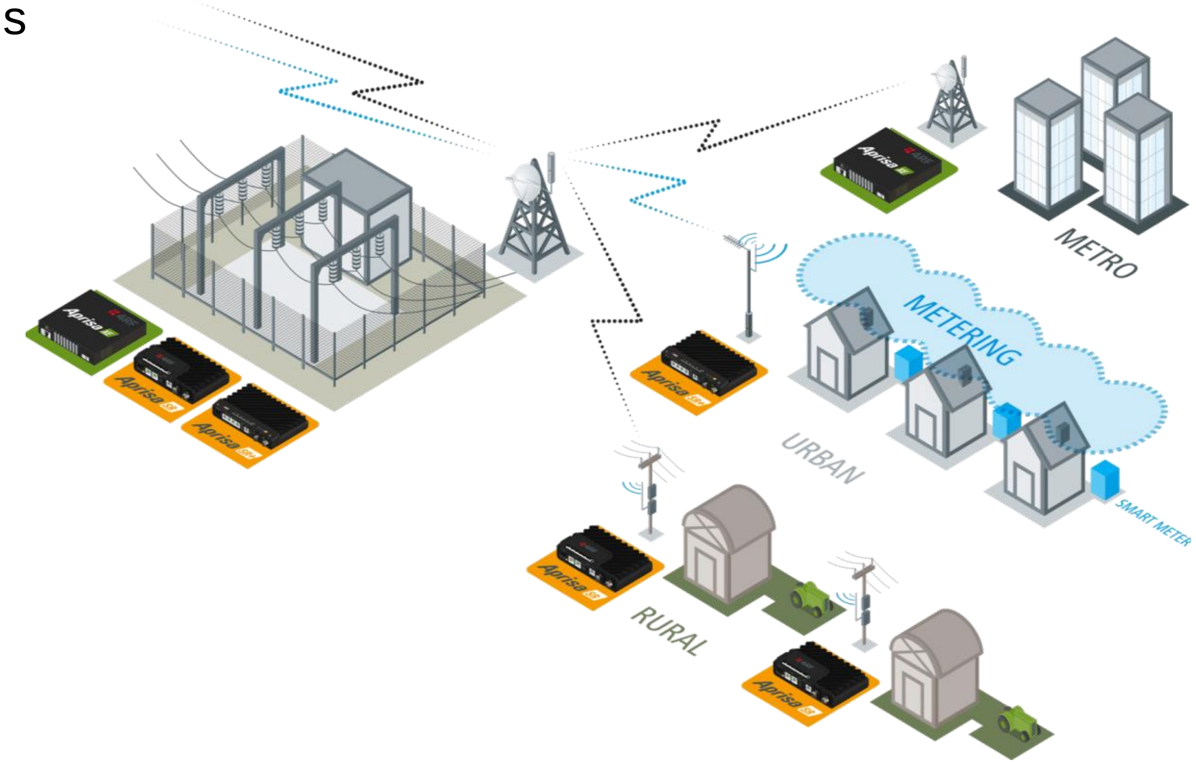
Tasks typically data gathering and remote control of machinery

Distances are typically in the range 5 to 75 miles, sometimes more

Number of remotes can vary from hundreds to thousands

Communication options

- Private radio VHF/UHF SCADA
- Unlicensed spread spectrum
- IEEE 802.16s
- CAT-M / NB-IoT
- LTE



What are the options?

What do distribution automation (DA) grid devices need?

Utilities Technology Council™

FORT WORTH UTC TELECOM & TECHNOLOGY

DA grid device categories

Tier 1 – very low latency and requiring high availability

- Feeder protection relays

Tier 2 – low latency < 2 seconds and high priority

- Recloser controllers
- Fuse savers (lateral line vacuum circuit breaker)
- Capacitor banks controllers
- Fault circuit indicators

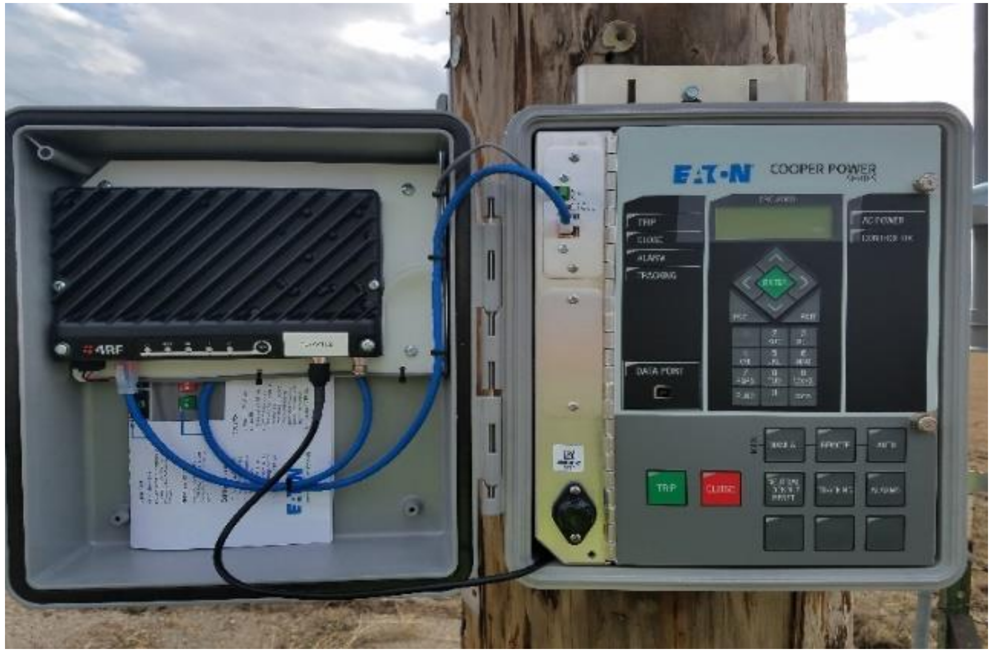
Tier 3 – not latency critical and requiring medium to high capacity

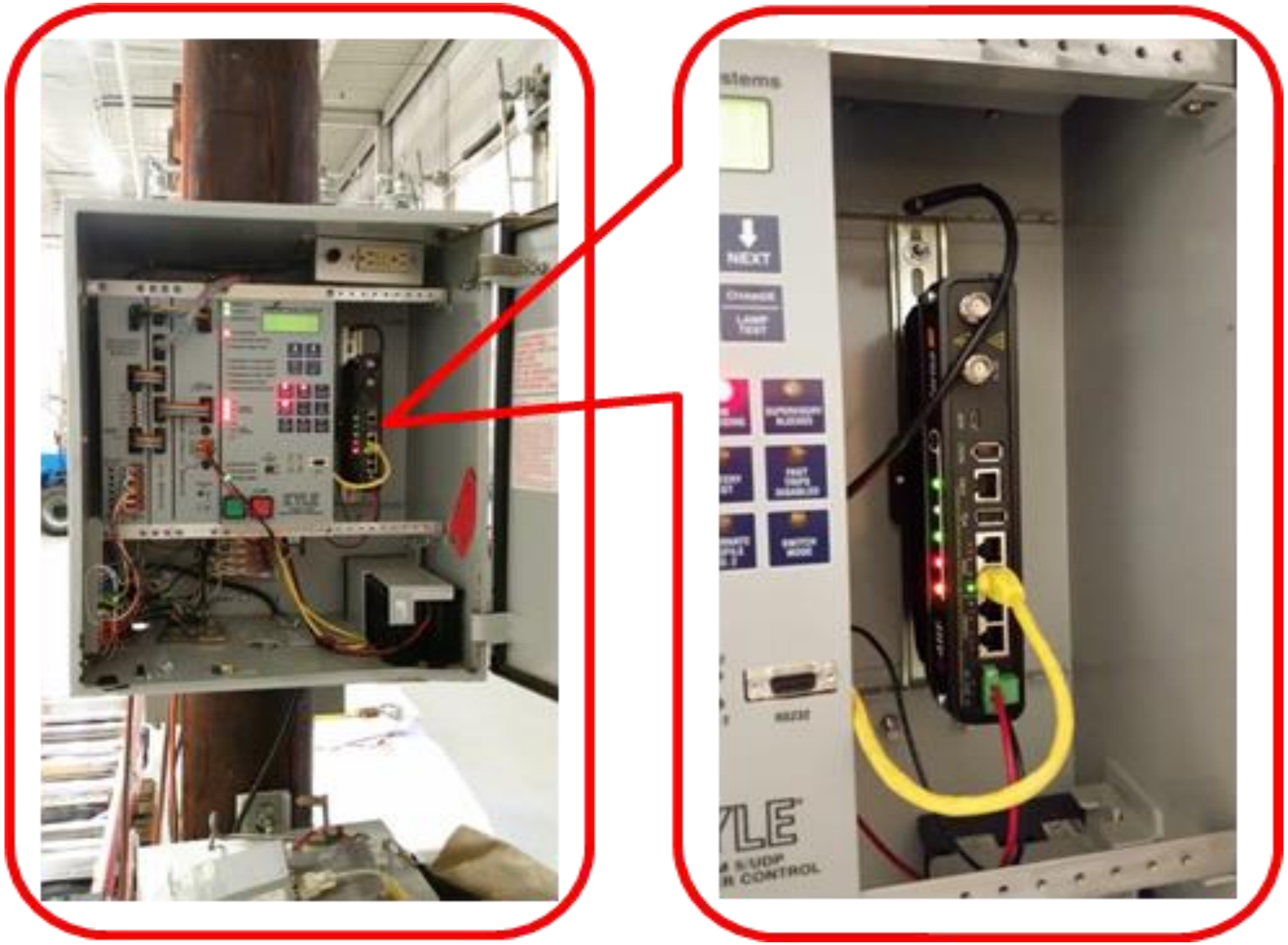
- Metering system backhaul
- GUI remote configuration of Tier 1 and 2 grid devices
- Mobile field force productivity included in this category

UTC Utilities Technology Council™

FORT WORTH UTC TELECOM & TECHNOLOGY

DA device remote examples





FAN technology comparison

Metric	VHF/UHF SCADA	Unlicensed Radio	Public LTE	NB-IoT	CAT-M
Dedicated spectrum needed?	No VHF/220/UHF	No 900 MHz	Yes 1.4 – 20 MHz	Usually 200+ kHz	Yes 1.4 MHz
Speed	60 – 500 kbps	60 – 500 kbps	5 – 100+ Mbps	50 – 75 kbps	375 kbps – 1 Mbps
Latency	Low 10 – 50 ms	Variable	Variable	High 1.6 – 10 s	Low 10 – 15 ms
Priority	High	Variable	Variable	Medium	Medium
System cost	Low	Low	High	High	High
Terminal cost	Medium	Medium	Low	Low	Low
Security	Very high (vendor)	Variable	High	High	High
UE transmit power	High 37 dBm	High 30 dBm	Low 23 dBm	Low 20 / 23 dBm	Low 20 / 23 dBm
Reliability	High	Low	Variable	High	High
Deployment time	Low	Low	Variable	Variable	Variable
Recovery time	Low	Low	High	High	High
Standards	Few	None	Yes	Yes	Yes

Recommend for real time control and metering

Recommend for non-critical metering, GUI, and mobile workforce productivity

4RF

Utility communication technology vs device categories

Licensed

Tier 1 and Tier 2

- Low latency
- High availability
- High priority
- Medium data rates
- Long range
- Need hardening IEC and IEEE

Unlicensed

Some Tier 2

- Variable latency
- Medium availability
- Medium data rates
- Short range
- Not reliable over long distances
- Need hardening IEC and IEEE

LTE

Limited Tier 2 and Tier 3

- Public and private networks
- Variable latency
- Coverage limited
- High data rates
- High remotes volumes
- Need hardening IEC and IEEE

UTC Utilities Technology Council™

FORT WORTH UTC TELECOM & TECHNOLOGY

Utility communication technology trade-offs

Licensed

- Few credible vendors
- Requires detailed planning
- Capacity constrained by available frequencies
- Coverage easily engineered to suit application

Unlicensed

- Few credible vendors
- Frequencies shared with consumer devices
- Capacity constrained
- Coverage usually easily engineered to suit application
- Interference limited

LTE

- Public networks are shared
- Private networks are expensive
- Public network latency highly variable and not under control of utility
- Public network coverage poor in rural area
- Limited hardened LTE device offerings

The radio-based FAN – familiar but now improved

The re-invention in 2012 of sub 1 GHz high efficiency narrow channel radio via the introduction of QAM modulation to deliver much needed FAN capacity is a classic example of competition driving innovation

Commonly accepted wisdom that **standardized** solutions are always 'best'

- Standardization of interconnection interfaces are crucial but this requirement does not extend to the air interface unless lowest common dominator performance is acceptable

Critics say narrow channel radios do not have capacity and that **more complex radios systems** are required to address FAN needs

- Faster than 802.16s, much faster than NB-IoT
- More bps per hertz than multicarrier technologies TDD/FDD single frequency and two frequency
- Point to multipoint needs sophisticated access control built into air interface
- Narrow RF channels now deliver near broadband speeds

FAN – speed vs throughput

Datasheet values vs real world, think testing

Net throughput or ‘goodput’ shown, 2x this with compression

Need to factor protocols to be used in throughput evaluation

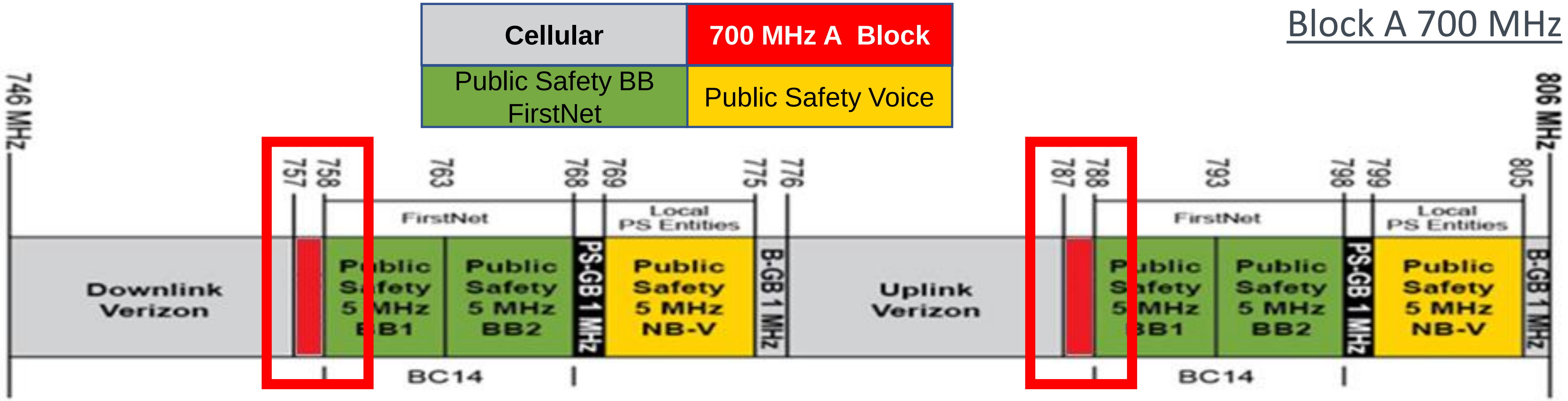
More carriers = more capacity but needs better re-use

ATPC and ACM = increases re-use

Metric @ 64 QAM	100 kHz	50 kHz	25 kHz	12.5 kHz
Raw speed	400 kbps	240 kbps	120 kbps	60 kbps
Throughput	UL 163 kbps DL 233 kbps	UL 98 kbps DL 140 kbps	UL 41 kbps DL 57 kbps	UL 27 kbps DL 37 kbps

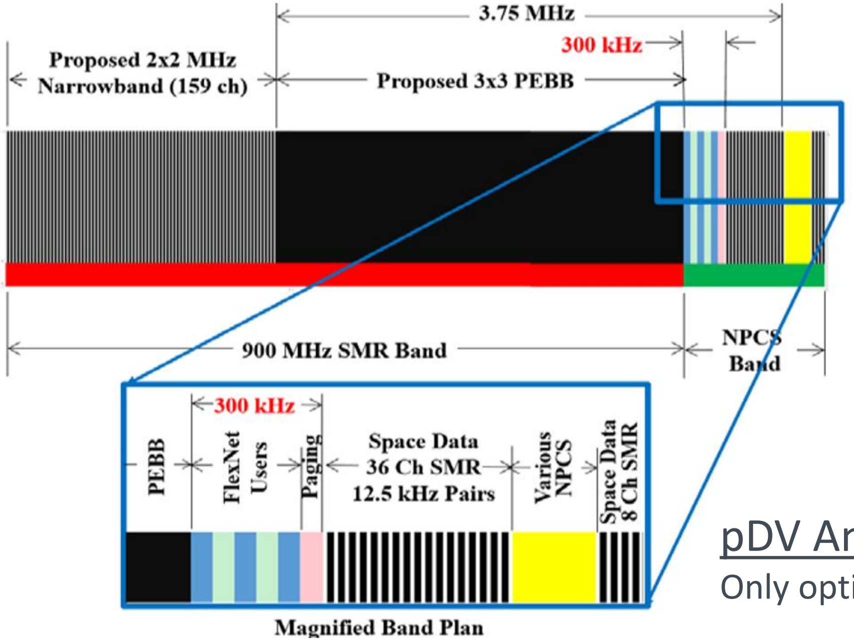
Available private spectrum – 700 and 900 MHz options

Block A 700 MHz



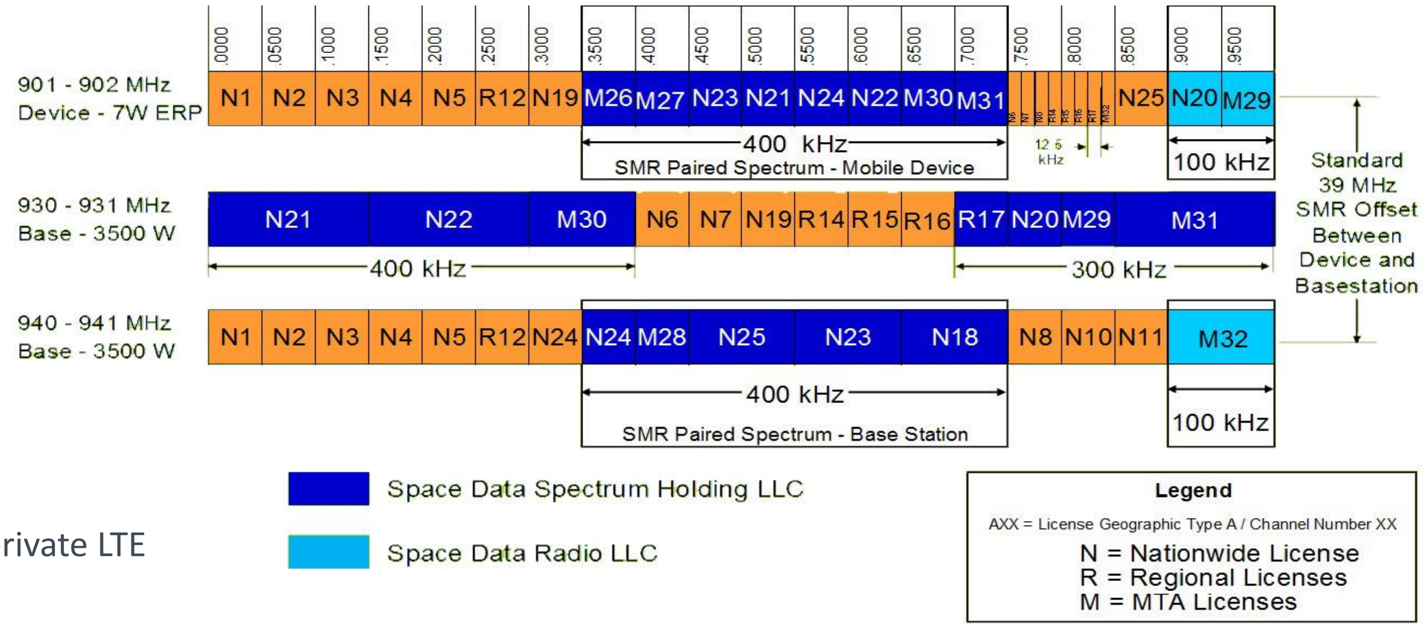
Cellular	700 MHz A Block
Public Safety BB FirstNet	Public Safety Voice

Space Data 900 MHz



pDV Anterix

Only option for <1 GHz private LTE



.0000
.0500
.1000
.1500
.2000
.2500
.3000
.3500
.4000
.4500
.5000
.5500
.6000
.6500
.7000
.7500
.8000
.8500
.9000
.9500
901 - 902 MHz
Device - 7W ERP
N1 N2 N3 N4 N5 R12 N19 M26 M27 N23 N21 N24 N22 M30 M31 N6 N7 N8 R14 R15 R16 R17 M32 N25 N20 M29
400 kHz
SMR Paired Spectrum - Mobile Device
12.5 kHz
100 kHz
930 - 931 MHz
Base - 3500 W
N21 N22 M30 N6 N7 N19 R14 R15 R16 R17 N20 M29 M31
400 kHz
300 kHz
940 - 941 MHz
Base - 3500 W
N1 N2 N3 N4 N5 R12 N24 N24 M28 N25 N23 N18 N8 N10 N11 M32
400 kHz
SMR Paired Spectrum - Base Station
100 kHz
Standard 39 MHz SMR Offset Between Device and Basestation
Space Data Spectrum Holding LLC
Space Data Radio LLC
Legend
AXX = License Geographic Type A / Channel Number XX
N = Nationwide License
R = Regional Licenses
M = MTA Licenses

Radio based FAN spectrum summary

700 MHz **Upper Block A** spectrum arranged as 2 by 1 MHz bands

- 757–758 MHz downlink
- 787–788 MHz uplink

901–902 / 930–931 / 940–941 MHz **Space Data** 3 by 1 MHz (with some existing use)

896–901 / 935–940 MHz (Band 8) **pDV Wireless now Anterix** and will be sought after for LTE

FCC **Part 90** LMR and **Part 101** MAS bands

- VHF, 220, 450, 900 MHz

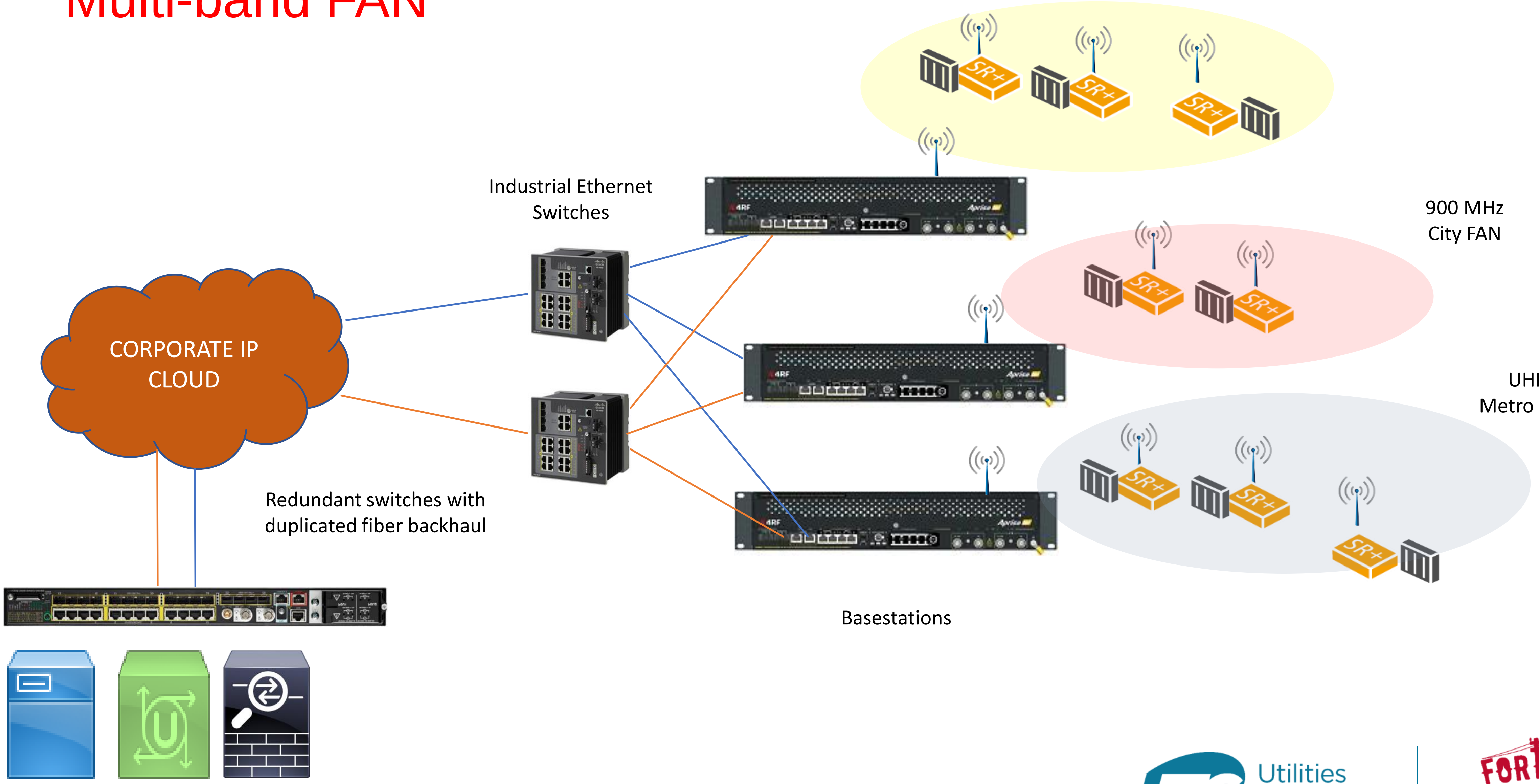
Part 22 re-purposed paging allocations at 220 and 900 MHz

Part 80 re-purposed marine VHF (inland only)

Many utilities utilize multiple bands to harness advantages of range (low frequencies like VHF and 220 MHz) and capacity (higher frequencies like 700 and 900 MHz) – the **multi-band FAN**

Multi-band FAN

4RF



VHF Rural FAN

Industrial Ethernet Switches

900 MHz
City FAN

CORPORATE IP CLOUD

UHF
Metro FAN

Redundant switches with duplicated fiber backhaul

Basestations

Utilities Technology Council™

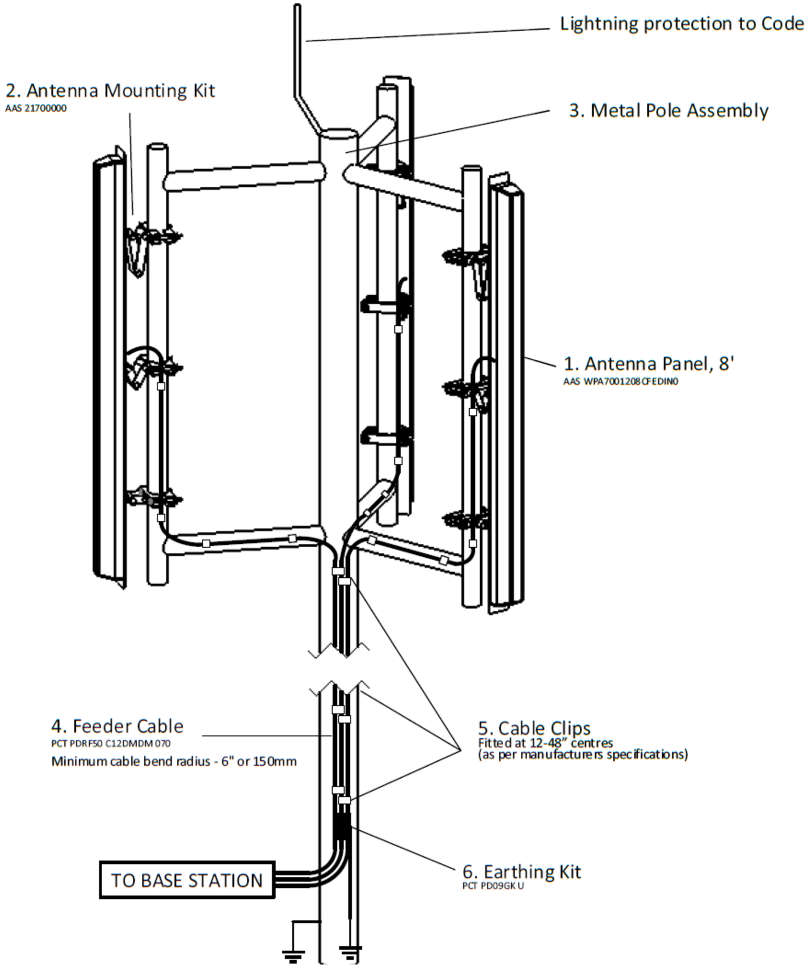
FORT WORTH
UTC TELECOM & TECHNOLOGY

Example of new high density networks at 700 MHz

FAN not ‘cellular’ but cell based

Sectored installation – gain and speed for 700 and 900 MHz

Master vs remote – antenna cost balance

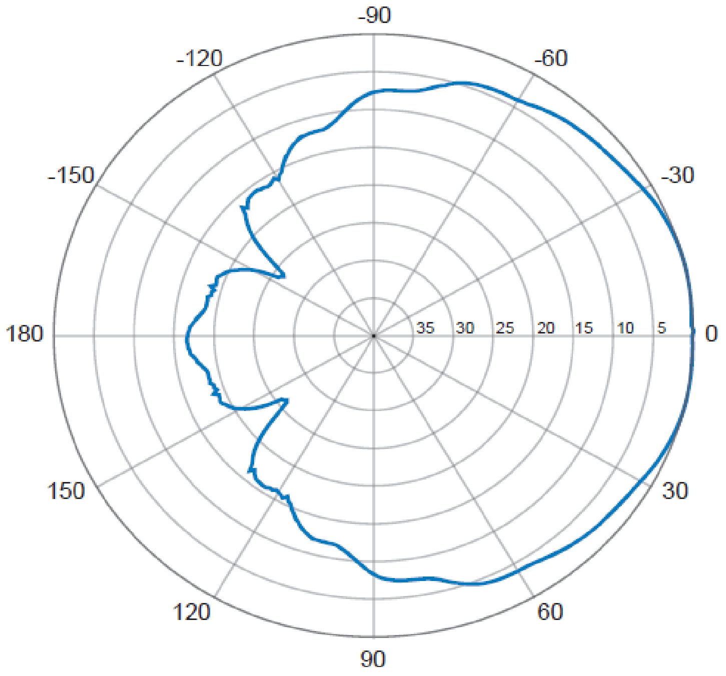


Typical panel antenna pattern covering 700 and 900 MHz

Typical three sector or high density four sector arrangements, downtilt option

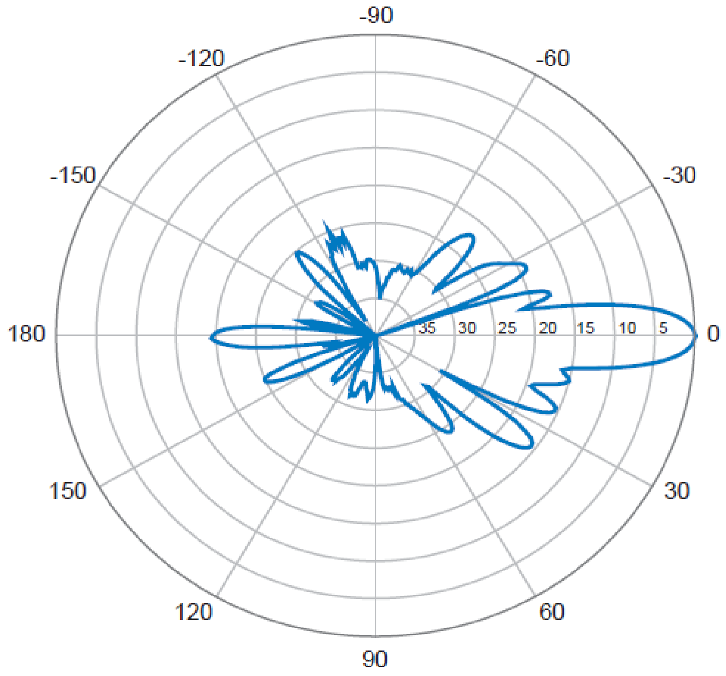
Beam = 102° @ -3 dB, 95”, wideband 16.1 dBi @ 700 MHz Block A, 16.6 dBi @ 900 MHz MAS

WPA-700102-8CF-EDIN-X



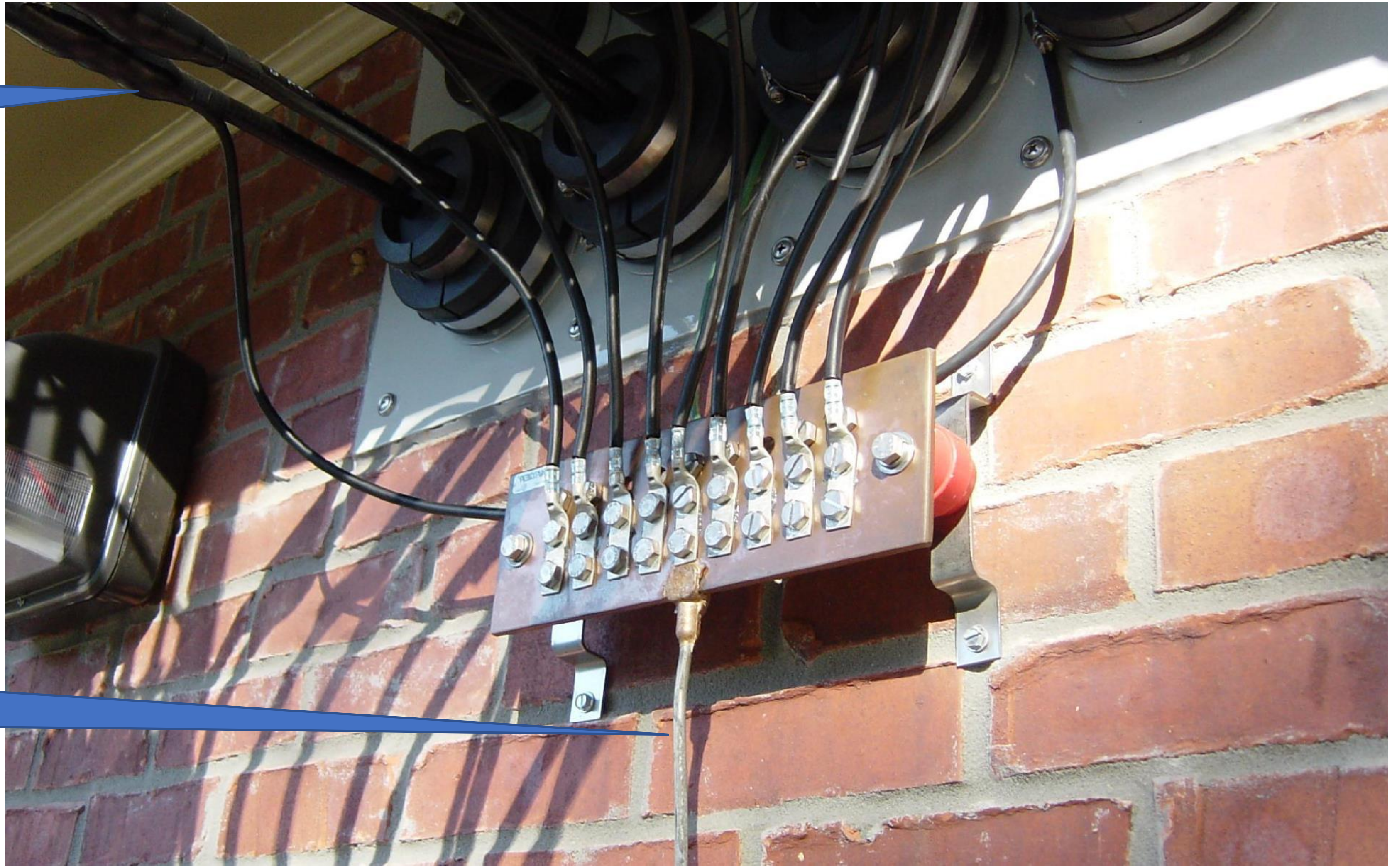
Horizontal | 750 MHz

WPA-700102-8CF-EDIN-0



0° | Vertical | 750 MHz

Earthing at building entry – minimum

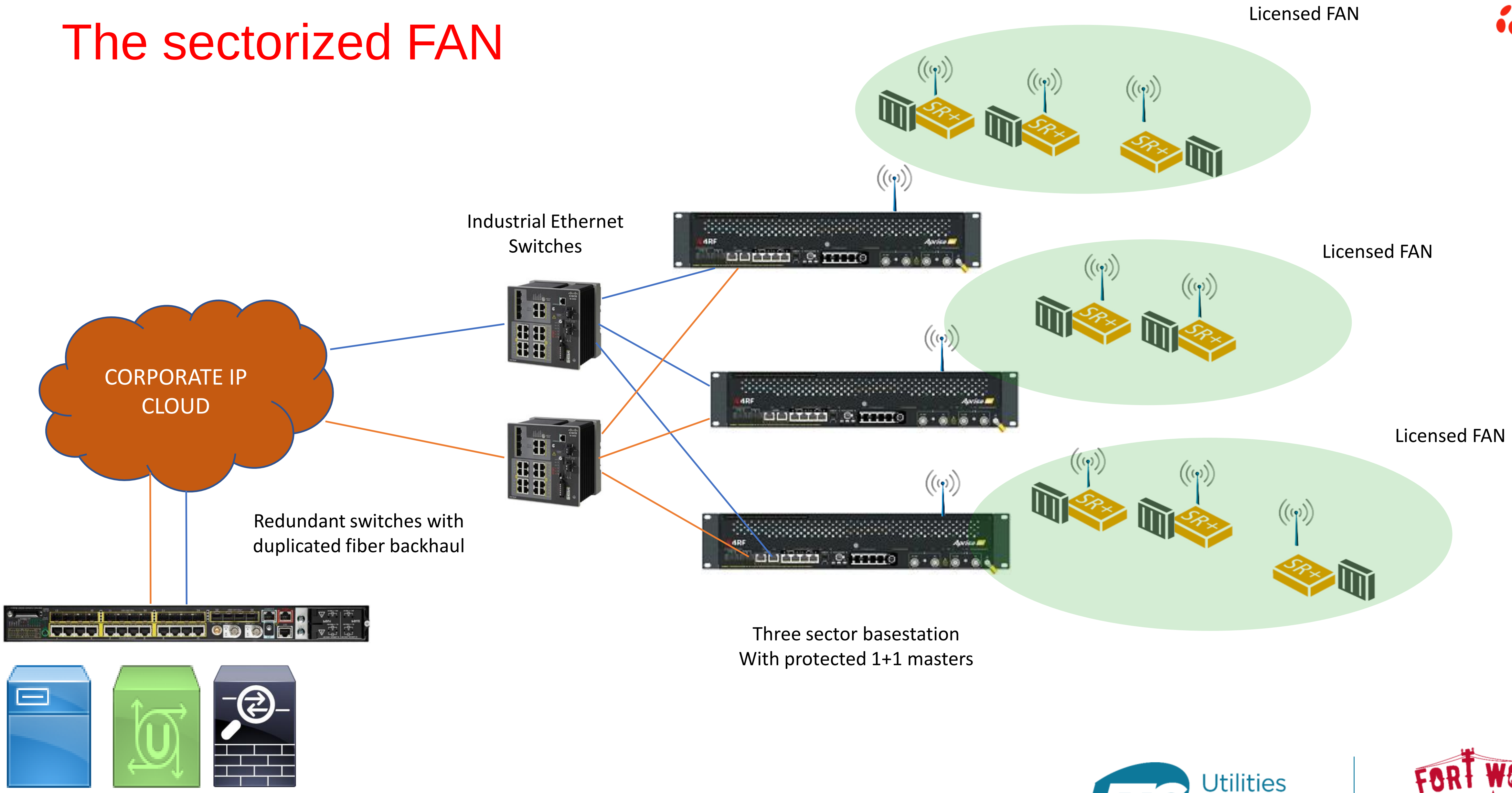


Earth kit applied to cable with waterproof protection applied

Critical to waterproof all antenna and feeder connections for long life

Earth plate to ground ring via heavy copper

The sectorized FAN



Licensed FAN

Industrial Ethernet Switches

Licensed FAN

CORPORATE IP CLOUD

Licensed FAN

Redundant switches with duplicated fiber backhaul

Three sector basestation With protected 1+1 masters

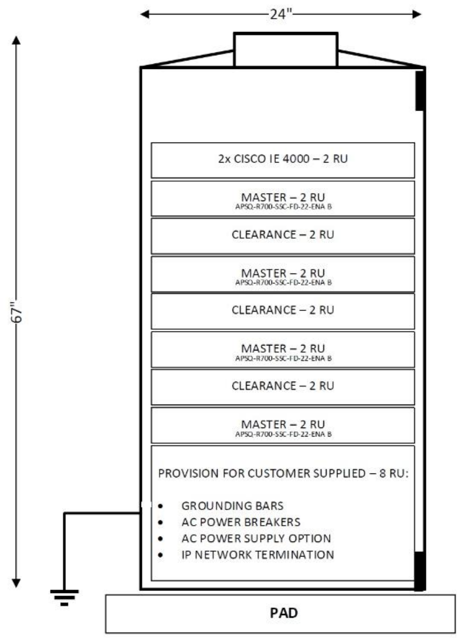
Utilities Technology Council™

FORT WORTH
UTC TELECOM & TECHNOLOGY

Installation three sector and three sectors with two carriers

Base station and master radios

- Three sector site and six master sites shown



24"

67"

2x CISCO IE 4000 – 2 RU

MASTER – 2 RU
APSQ-R700-SSC-FD-22-ENA B

CLEARANCE – 2 RU

MASTER – 2 RU
APSQ-R700-SSC-FD-22-ENA B

CLEARANCE – 2 RU

MASTER – 2 RU
APSQ-R700-SSC-FD-22-ENA B

CLEARANCE – 2 RU

MASTER – 2 RU
APSQ-R700-SSC-FD-22-ENA B

PROVISION FOR CUSTOMER SUPPLIED – 8 RU:

- GROUNDING BARS
- AC POWER BREAKERS
- AC POWER SUPPLY OPTION
- IP NETWORK TERMINATION

PAD

Example Cabinet, APX RM672430 – Overall dimensions 67" x 24" x 30"
Fixing Centres 15" x 25", Max fixing diameter 3/4"
NEMA 3R/NEMA 4X cabinet

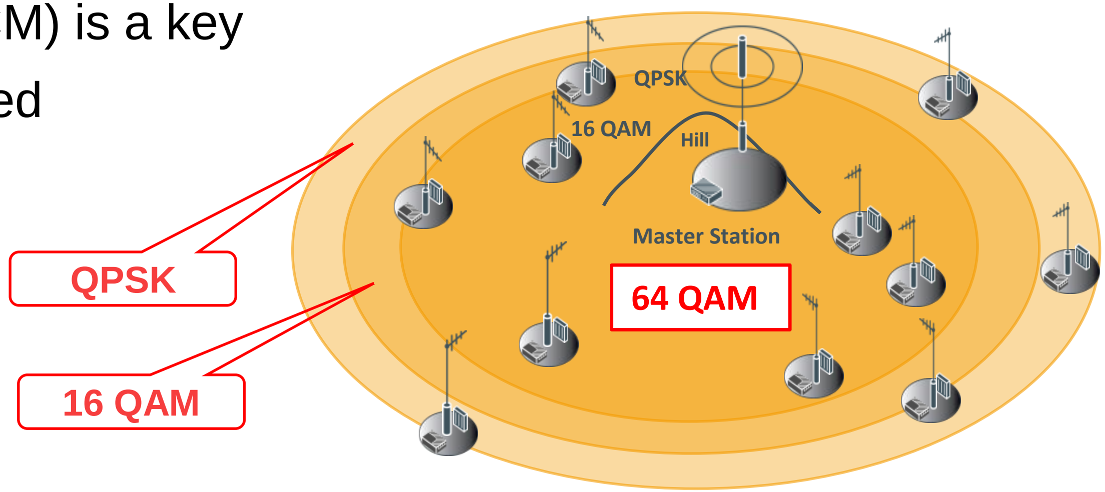
4RF Title Aprisa SR+ 3 Master Base Station
Pedestal mounted – 1 Standard Cabinet

Drawing Number	Revision	Release Date
RFP-M03-1-1	01	26/09/16

ACM making best use of the channel

The ability to provide adaptive coding and modulation (ACM) is a key feature, both uplink and downlink ACM should be supported

- Enables maximum use of channel
- Highest speed for near remotes
- Robust connectivity for far remotes

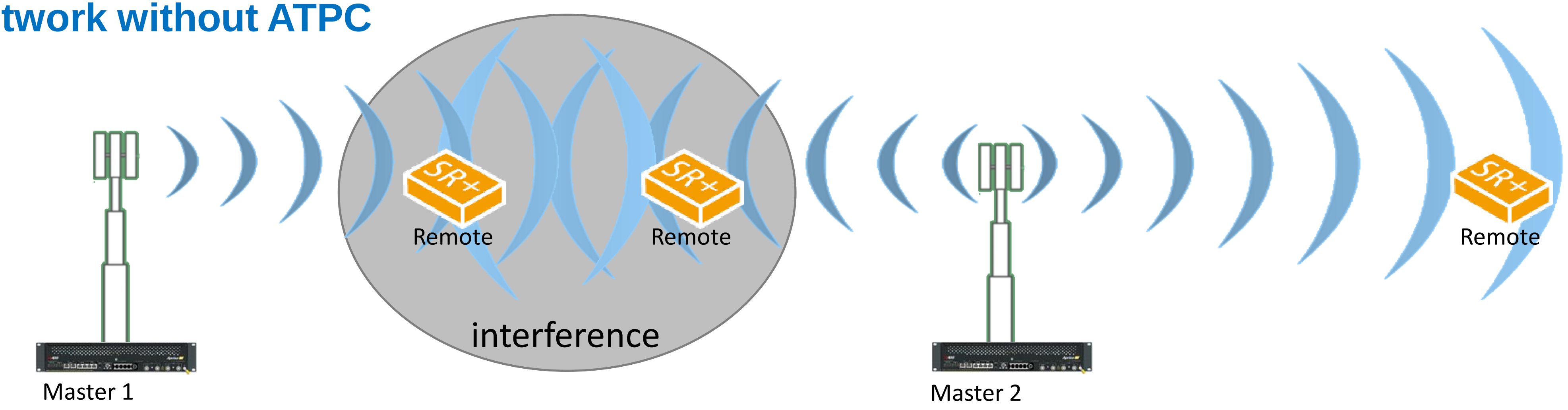


Allows reduced operational fade margins – plan with standard fade margin for robust QPSK but enjoy operational time at high capacity 64 QAM

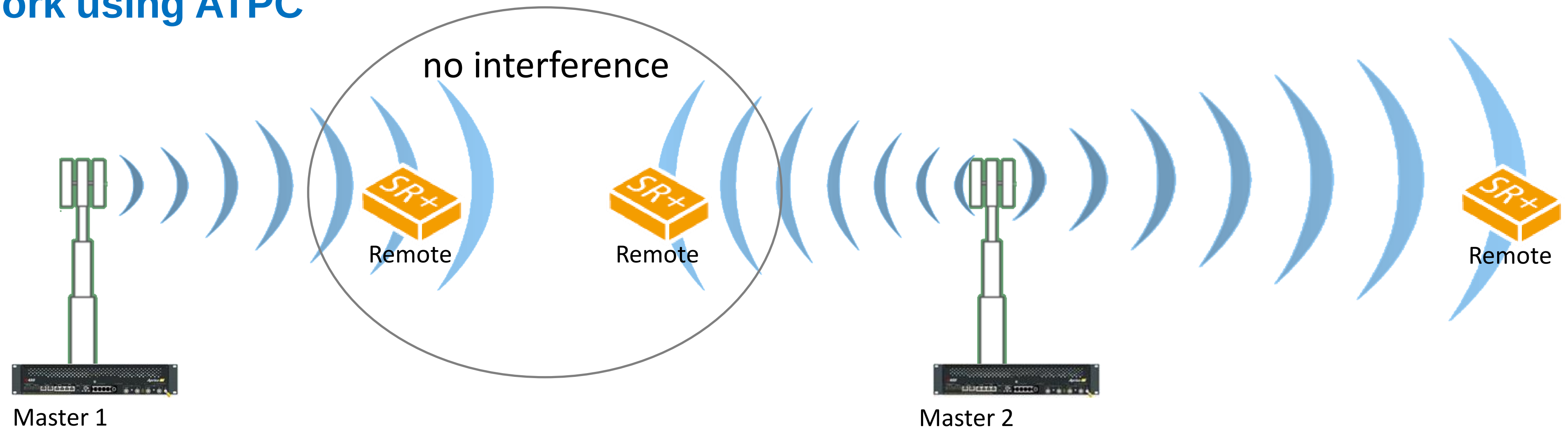
- Maintains link operation during fading, multipath, and interference scenarios
- ACM based on SNR performance and errored packets

ATPC reduces noise and interference, increasing re-use

Network without ATPC

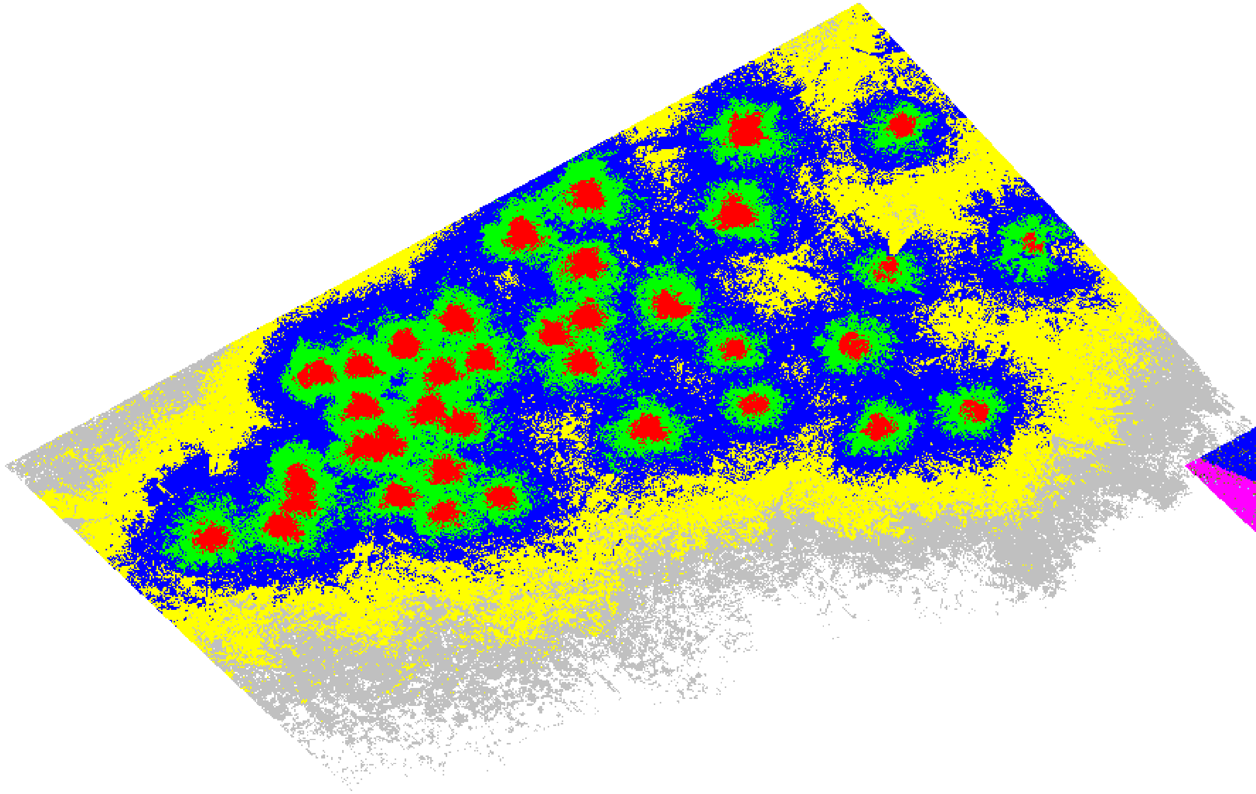


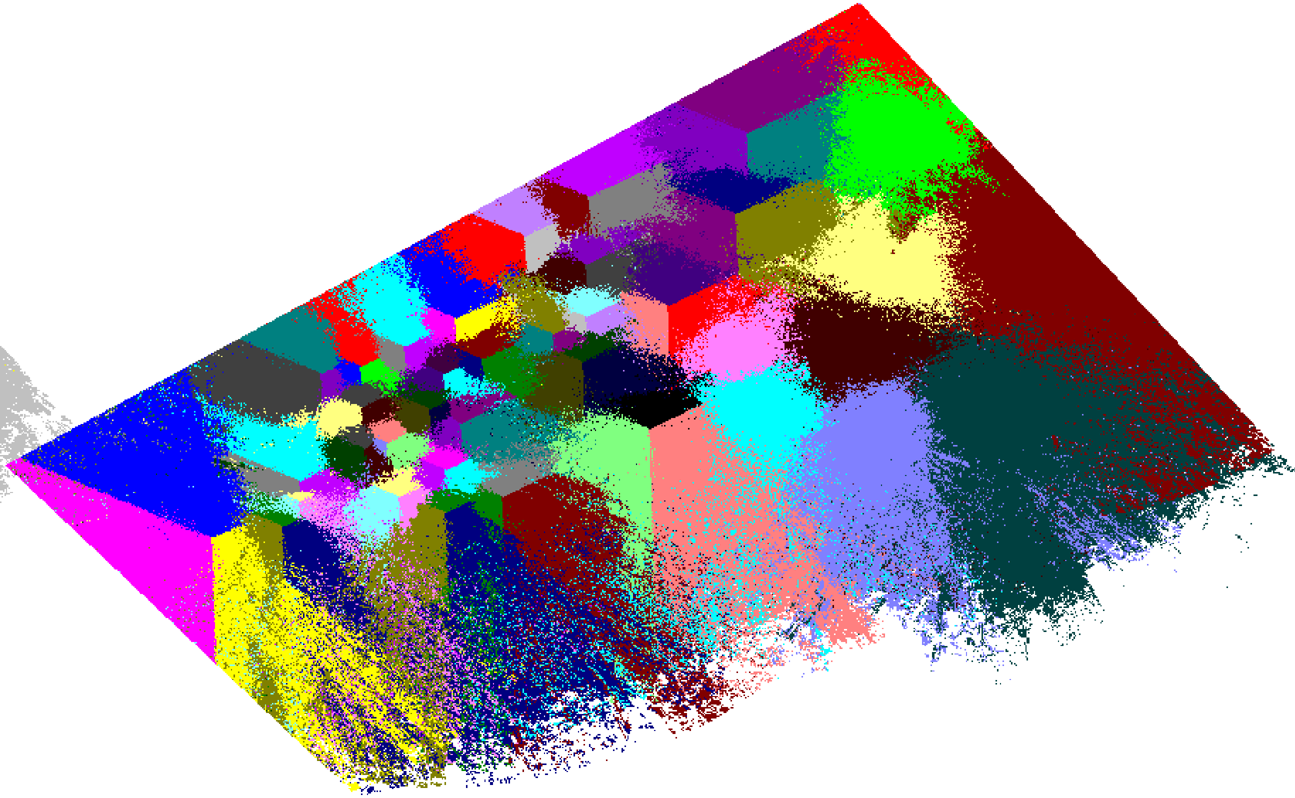
Network using ATPC



Omni vs sector – 38 remotes at ground level and masters at 60’

Frequency re-use critical





Best server plot – color = frequency and sector coverage

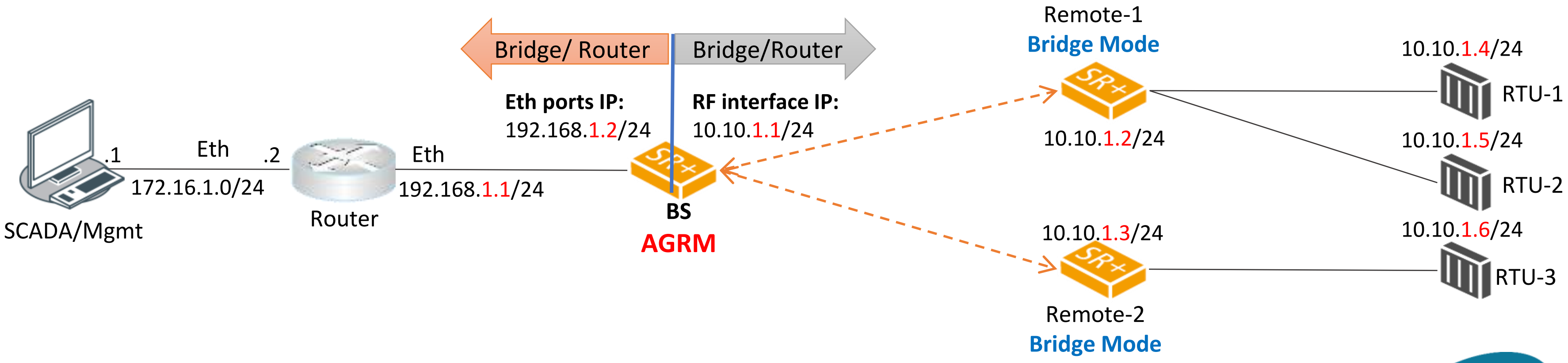
Advanced IP router mode features in FAN

Combined IP Layer 2 and Layer 3 features for IP fan deployments

- Simplified RTU IP configuration
- All remote RTU devices remain in same L2 bridge subnet
- Base station backhaul is in a different subnet

Makes FAN backhaul connection to SCADA master via corporate IP network easier

Isolation of Ethernet broadcast domains – corporate LAN/router (backhaul) and FAN Radio LAN domains



Utilities Technology Council™

FORT WORTH UTC TELECOM & TECHNOLOGY

Platform multi-service support

Single platform – multiple services

- Port per application
- VLAN for virtual separation
- QoS for optimization
- Throughput requirements easily met

Port 2 – AMI

Port 1 – Smart Grid

Radio platform is ready for immediate or future multi-service implementation – typical used immediately or as a future proof option for utilities

FAN packet processing

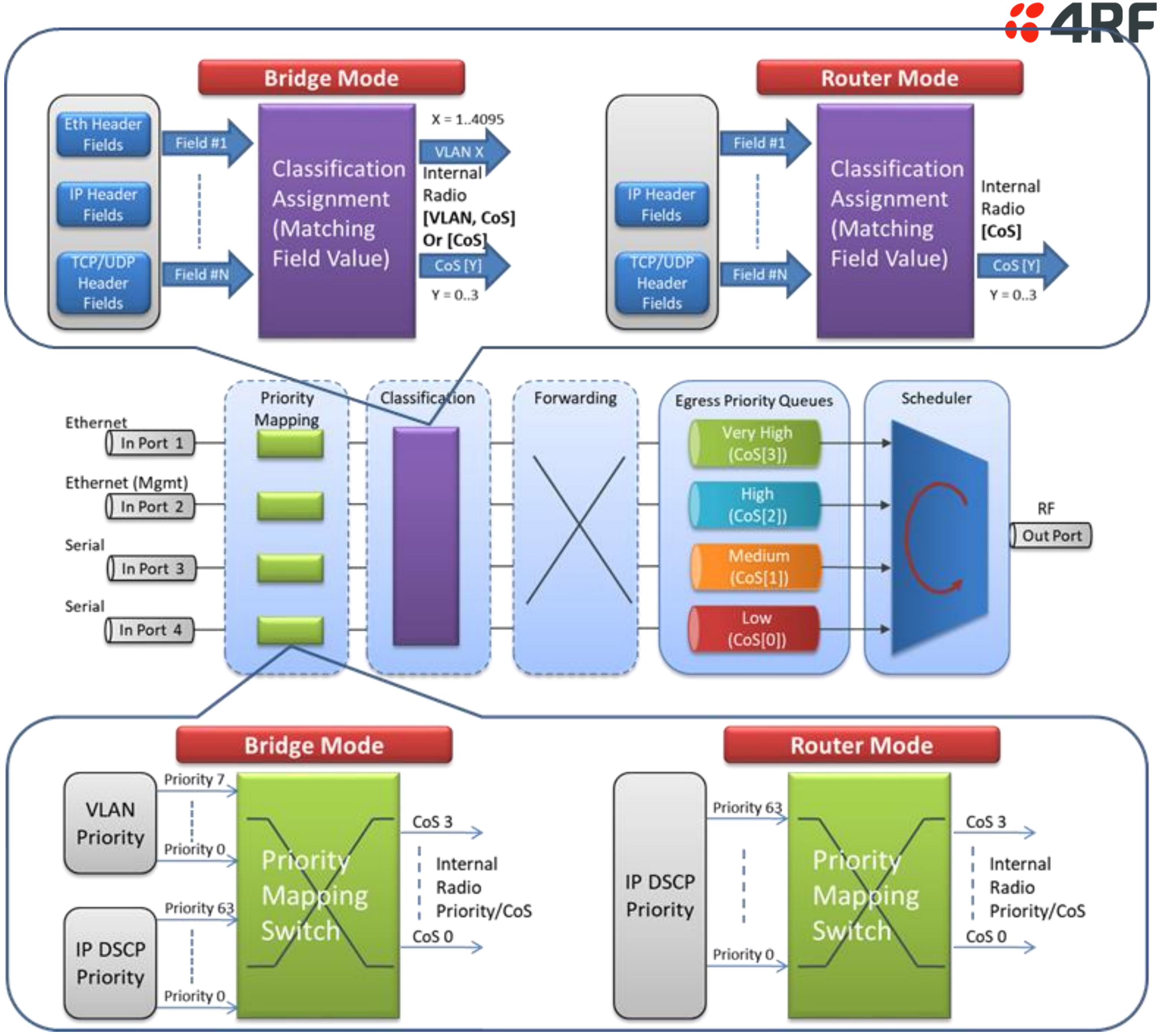
Multiple priority queues

Flexible port mapping or QoS driven

ARP cache and IP header compression

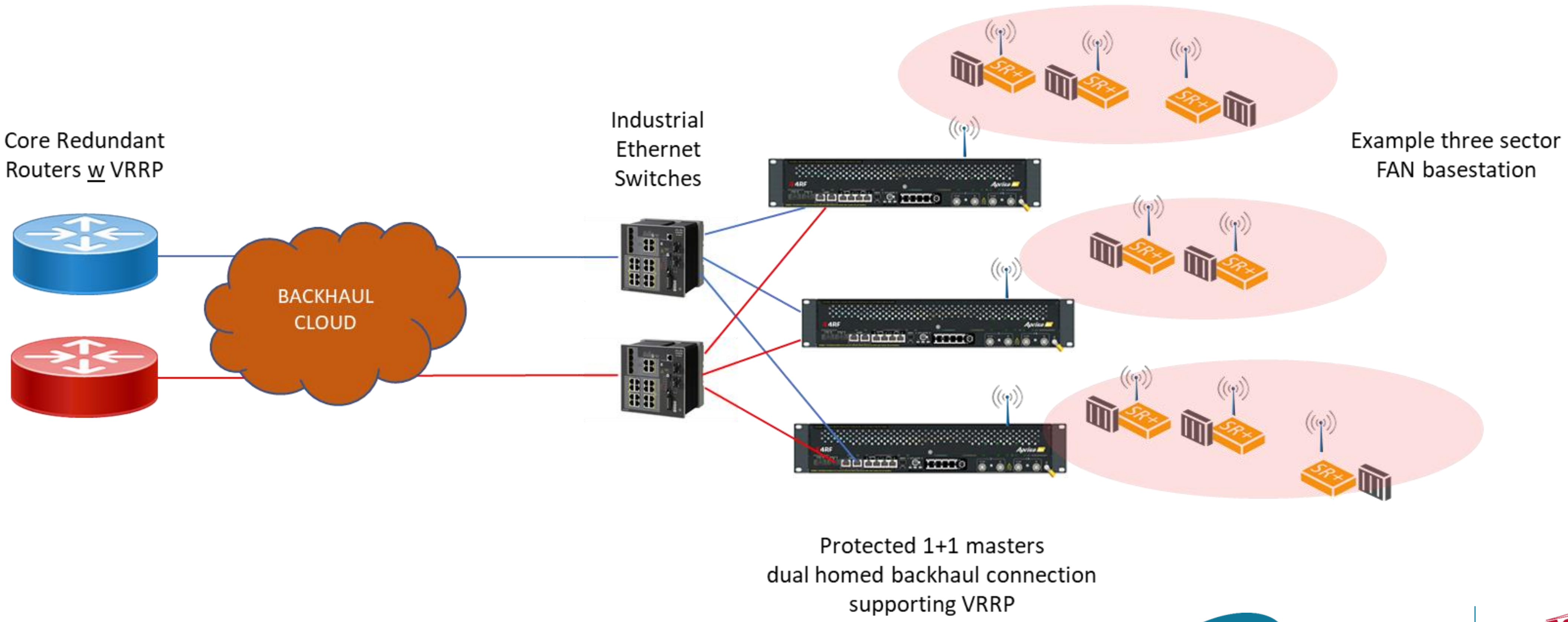
IP from edge to core, with serial TS

- Serial RTU and IED support
- Simplicity, flexibility, and depth
- Security with AES, CCM, and OTAR
- SNMP, CLI, and web management
- Essential tools, filter unwanted traffic
- Layer 2 VLAN aware, tagging and Q-in-Q



Dual homing backhaul protection with VRRP

Allows backhaul route failover



Core Redundant Routers w VRRP
BACKHAUL CLOUD
Industrial Ethernet Switches
Example three sector FAN basestation
SR+
Protected 1+1 masters dual homed backhaul connection supporting VRRP

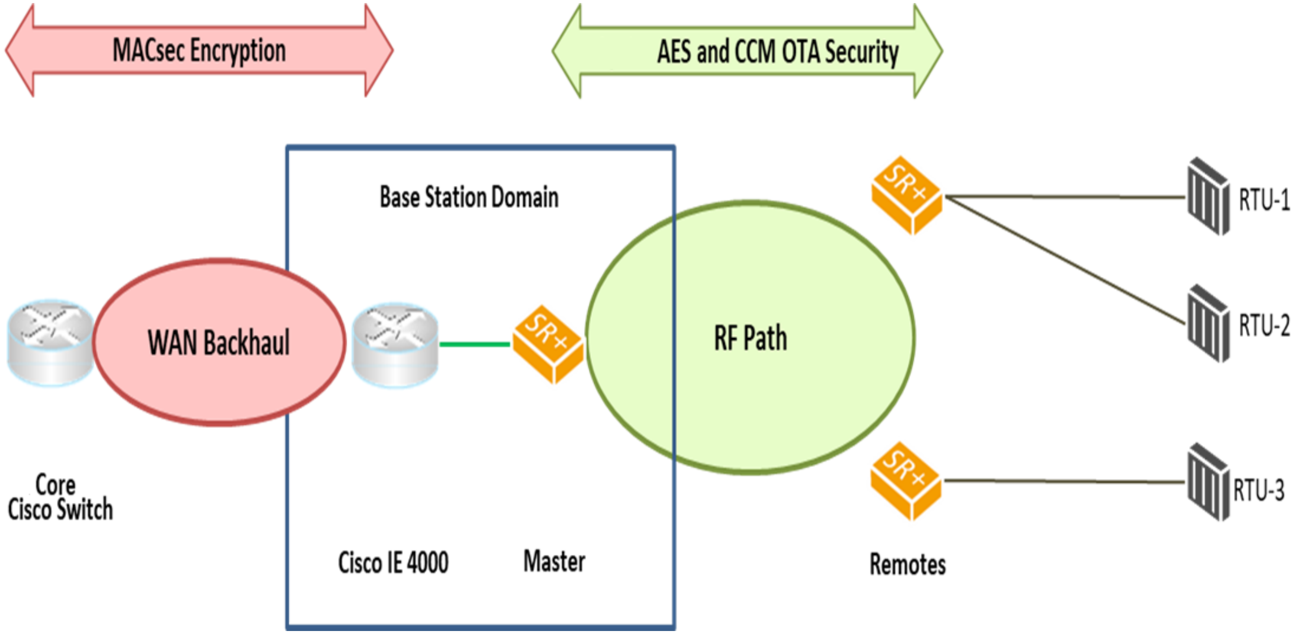
Security domains

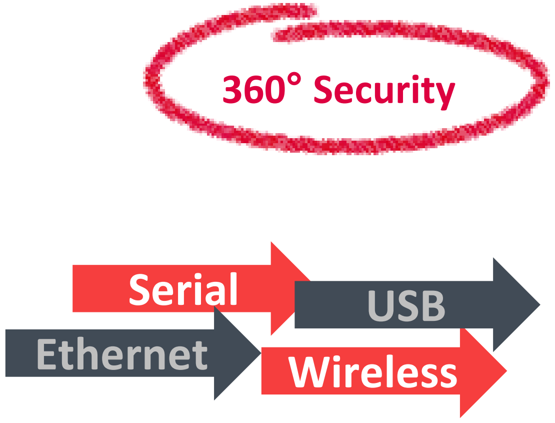
Over-the-air encryption provides low-overhead on radio access network

Security profile established at setup and distributed OTA to all remotes

Logging of security related events, 360 degree event consideration

L3 IPSEC or L2 MACsec WAN backhaul security





Over-the-air Symmetric Encryption

Encryption is used to reduce information leakage

Robust cryptographic algorithm important, today this is AES

Key is symmetric, same key used to decrypt and encrypt

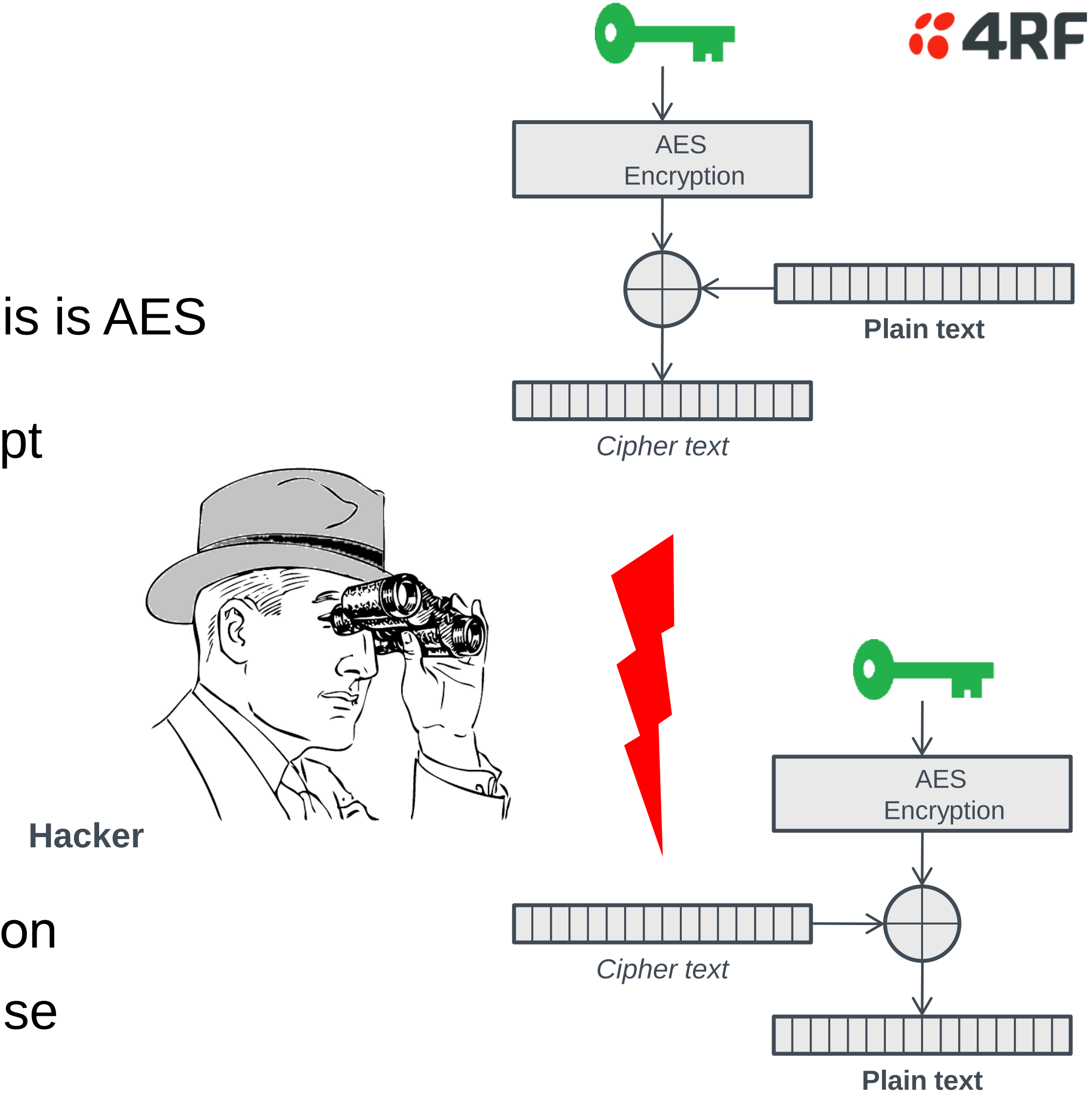
AES 128 bit block with 128, 192, or 256 bit keys

Security based on algorithm and shared secret key

Algorithm is public so key must be secret

Why change the key?

- Repetitive traffic increases ‘depth’ weakens protection
- **Regularly changing key** guards against compromise
- So we need a means to distribute new keys



Message Authentication – CCM CBC MAC

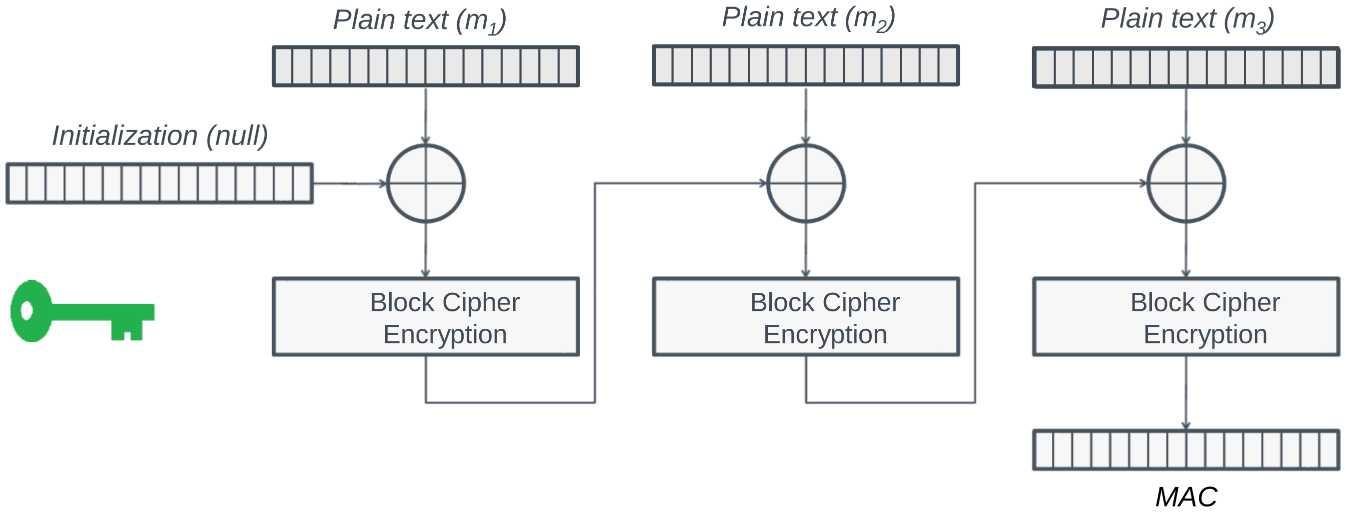
Counter mode encryption with cypher block chaining message authentication

CCM CBC MAC method with AES block cipher = AES (NIST SP 800-38C / RFC3610)

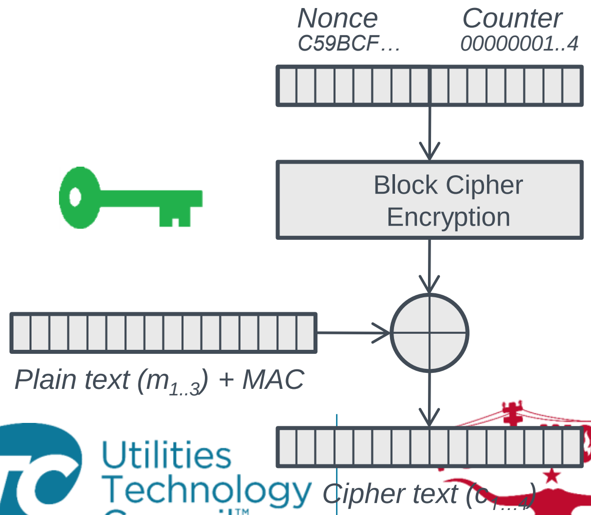
Message authentication code (MAC) then optionally encrypt

Send unique MAC with message for checking by receiver

- Creates unique message ‘fingerprint’



Note: diagram simplified as process is repeated once for each message plus MAC



Certificates and Post-quantum Cryptography

Quantum computing will eventually threaten many methods used to provide public/private key methods used to establish trust and exchange symmetric algorithm keying material

- Examples are RSA and ECC (elliptic-curve cryptography)

NIST Post-Quantum Cryptography Standardization Process underway, 26 candidate methods

- About 1/3 based on ring theory lattice modules, 1/3 linear code based, 1/3 on other methods

Watch this space

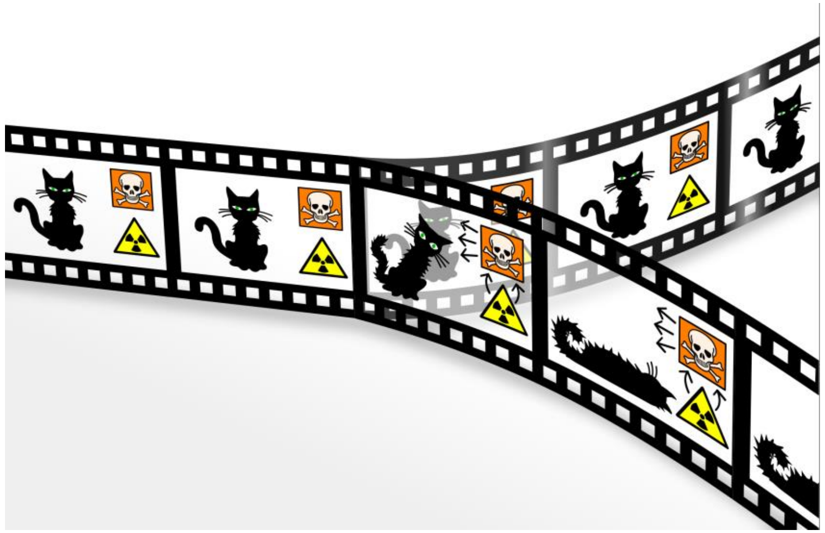
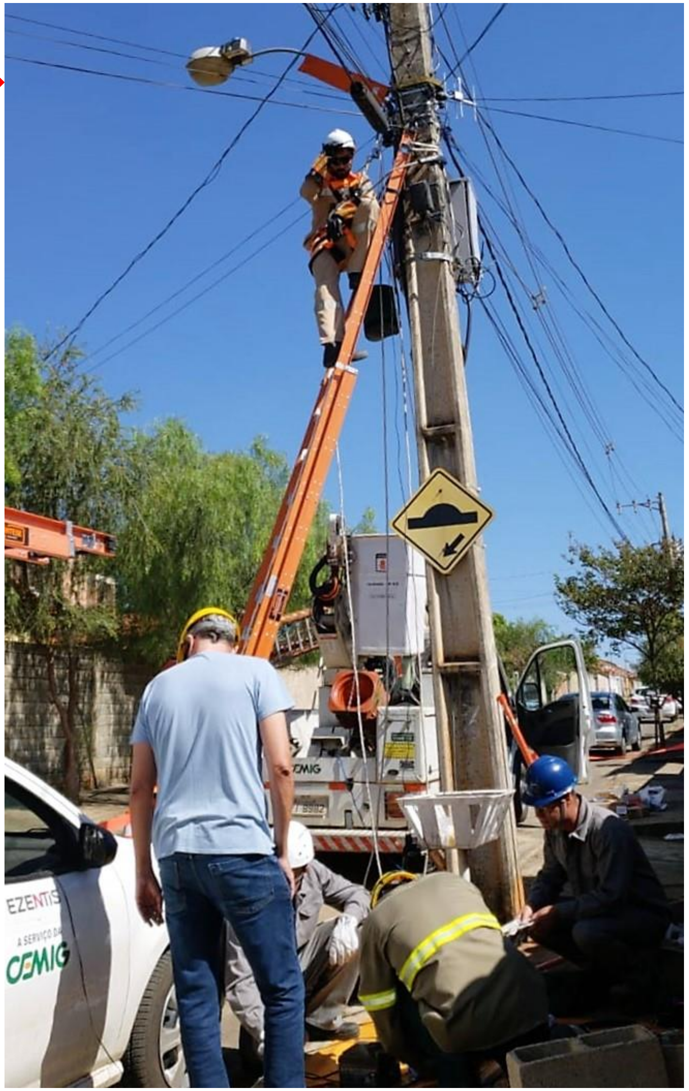


Image Christian Schirm

Utilitity deploymemts

Lab testing …

Installation



FAN deployments multi-band multi-application

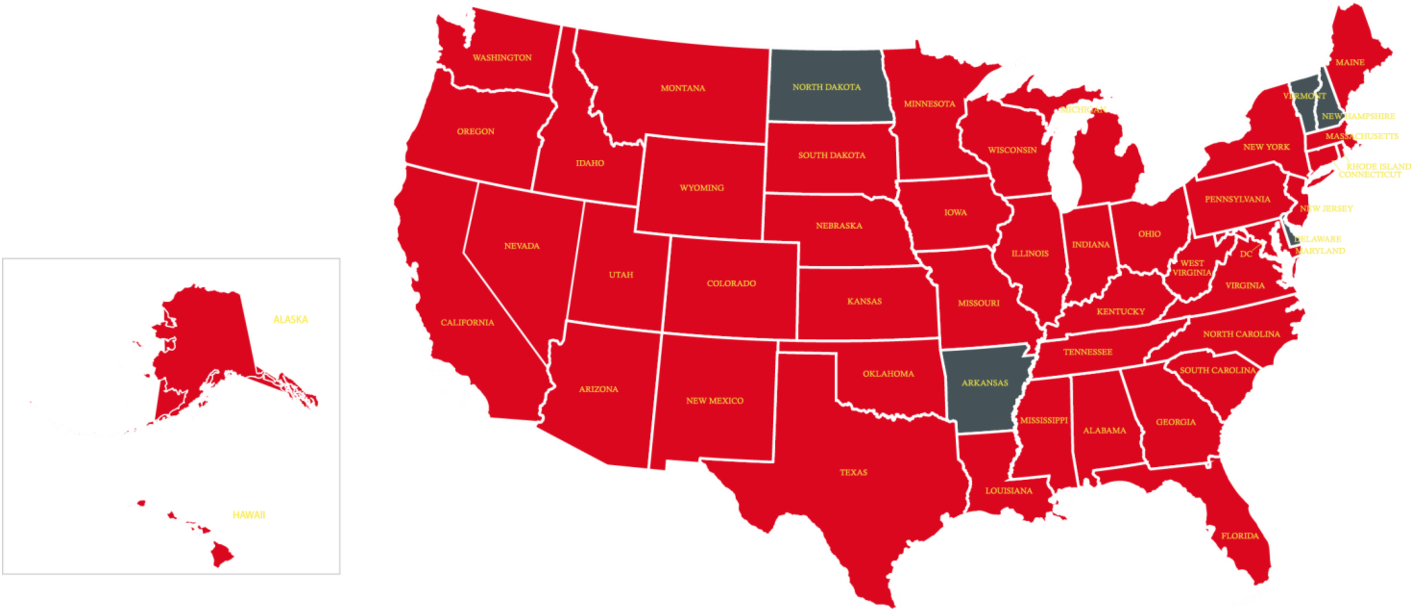
Spectrum – licensed VHF to 900 MHz and unlicensed 902-928 MHz

- Multi-band FAN

DA needs and FAN capacity – radio based FAN and LTE

- Multi-application FAN
- Antennas and lightning protection

Serial, IP and security features



Utilities Technology Council™

FORT WORTH UTC TELECOM & TECHNOLOGY

4RF™