Standards to Promote Interoperability

U.S.-Africa Clean Energy Standards Program

Yuval Hanan
Region Manager East Africa
Motorola Solutions
GM Motorola Solutions Rwanda

1st October-2018
ENSURING SAFER MORE PRODUCTIVE ELECTRICAL UTILITIES
Agenda:

1. Mission Critical Communications for Electrical Utilities
2. Mission Critical communications for IIoT
3. Sample Application
4. IIoT and Cyber Attack
MISSION CRITICAL COMMUNICATIONS

WHAT IS DEFINED IN THE STANDARD?

- Group Communications + Multi Agency Collaboration
- Nationwide Scalability
- Immediate
- Secure
- Always Available
- Interoperability
- Mission Critical Data
- Rugged Devices
- Operational Accessories
What is APCO\P25?

ALL IN ONE Radio

Enhanced Functionality & Performance

Group Calls
Private Calls
Telephony Interconnect
Emergency Calls
Emergency Alarm
Messaging
Embedded GPS
Packet Data
Authentication
Bluetooth
Encryption
Direct Mode (Talk Around)
SAVE YOUR COMMUNITY AND KEEP YOUR PERSONNEL SAFE

REDUCE INCIDENT RESPONSE TIMES
Visually and audibly alert firefighters in the station to incident details. Remotely turn off stoves, lock up and monitor security when the station is empty.

ENSURE EVERYONE GOES HOME
While on scene, account for all personnel and monitor their equipment to ensure everyone gets out safely.

KEEP YOUR REMOTE EQUIPMENT OPERATING AT PEAK PERFORMANCE

INCREASE PRODUCTIVITY AND REDUCE DOWNTIME
Achieve greater operational control with the powerful process automation and expansive communication capabilities of SCADA RTUs seamlessly integrated across your operations.

OPERATE MORE INTELLIGENTLY
Purpose built Machine-To-Machine (M2M) modems transmit operational technology data across your ASTRO 25 system to enterprise applications, without incurring subscription fees from other networks.
Besides talk what do we use our communication platform for...

Regionally: Kenya, Ethiopia, Rwanda* chose to use the P25 Mission Critical Standard for Public Safety and for utility use...
GSM\CELLULAR NETWORKS ARE ONLY AVAILABLE IN PLACES WHERE $$$ COULD BE GENERATED (POPULATED AREAS) OFTEN NOT AVAILABLE IN RURAL AREAS AND PLACES WHERE OUR GRIDS RUN
Your mission critical operations depend on reliable voice PTT communications all the time, everywhere you operate. Why not demand the same reliability from your data service. You can depend on ASTRO 25 data the same as you already trust your ASTRO 25 PTT service for:

- Resiliency Against Service Disruptions
- Coverage Everywhere You Need It
- Security

SUPER STORM SANDY WHEN WILL IT OCCUR AGAIN?

DURING SUPERSTORM SANDY THERE WERE:

- 25% OF CELL SITES IN THE 10-STATE REGION OUT OF SERVICE
- 18 DAYS BEFORE CARRIERS RESTORED FULL SERVICE
- 0 PUBLIC SAFETY SYSTEMS ADVERSELY AFFECTED
MOBILE OPERATION PLATFORM BRINGS A COMMUNICATION SITE TO AREAS OUT OF COVERAGE OR THAT SUFFERED A DISASTER
Communication Systems Could be interconnected Regionally for collaboration just like a power grid is connected.

Taking it a step further…

A single regional investment could save utilities a huge budget on critical communication once a system is managed centrally for a region.
INTEGRATE DATA INTO YOUR ASTRO 25 VOICE SYSTEM

In an ASTRO 25 voice and integrated data system, data coexists with voice traffic over the same radio frequencies. The system dynamically reallocates channels to voice or data in real time as user demand requires – maximizing your use of available channels.

Voice has priority over data so data transmissions will not interfere with voice calls. In times of emergency, a site’s data resources are reallocated if the demand for voice becomes exceptional, providing extra voice capacity when it becomes essential.

- Identical footprint as voice
- Same site equipment
- Channels dynamically switch to voice or data based on user demands
- Project 25 (P25) standard-based
ADDRESSING THESE CHALLENGES REQUIRES THE
SEAMLESS MOBILIZATION OF INFORMATION AND CONTROL

ACHIEVE UNCOMPROMISING SAFETY
DRIVE INTELLIGENT PRODUCTION
WITH THE ASSURANCE OF ASSET SECURITY
TRANSFORM THE ELECTRICAL UTILITY ENTERPRISE BY SEAMLESSLY CONNECTING WORKFLOWS, PEOPLE AND PROCESSES TO REAL TIME INFORMATION ACROSS ANY NETWORK
What is IoT?

The Internet of Things

- Anything
  - Any Device
- Anytime
  - Any Context
- Any Place
  - Anywhere
- Any Path
  - Any Network
- Anyone
  - Anybody
- Any Service
  - Any Business
$ 4 TRILLION INDUSTRY
BY THE YEAR 2020, THERE WILL BE 50,000,000,000 connected devices, creating and sharing 40,000,000,000,000,000 GB worth of data across the Internet of Things.
ADVANCING SAFER AND MORE PRODUCTIVE ELECTRIC UTILITIES

GLOBAL ENERGY CONSUMPTION WILL RISE BY OVER 50% OVER THE NEXT 30 YEARS

$20.5 BILLION IN ELECTRICITY IS LOST IN TRANSMISSION AND DISTRIBUTION IN THE US

184% INCREASE IN ATTACKS AGAINST INDUSTRIAL CONTROL SYSTEMS FROM 2016 TO 2017
OPERATIONAL TECHNOLOGY
Devices that enable the physical control, automation and monitoring of field assets and equipment i.e. RTUs, PLCs, Intelligent Electronic Devices, Sensors, M2M Devices

REMOTE TERMINAL UNIT (RTU)
A SCADA device capable of local processing and control for automation of physical assets and equipment while also communicating information for remote monitoring and/or control

PROGRAMMABLE LOGIC CONTROL (PLC)
A SCADA device capable of local processing and control for automation of physical assets and equipment without communication

INTELLIGENT ELECTRONIC DEVICE
More application specific devices capable of control of assets and equipment i.e. capacitor bank controllers and cathodic protection rectifiers
INDUSTRIAL IoT
SOLUTION COMPONENTS

SCADA: SUPERVISORY CONTROL AND DATA ACQUISITION
Process automation used to centrally monitor and control equipment and assets such as motors, valves, pumps, relays, etc.

M2M: MACHINE-TO-MACHINE
Operational technology data connectivity and communication to expand your organizational view and control.

NETWORK OF NETWORKS
A combination of communication networks capable of working together to collect and communicate data across operations.

PARTNER SOLUTIONS
A wide-range of partners who are certified to develop, integrate and deploy Industrial IoT solutions across a variety of areas of expertise.
ADVANCING SAFER AND MORE PRODUCTIVE ELECTRIC UTILITIES

- GENERATION STATION
- RECEIVING STATION
- DISTRIBUTION STATION
- END USER CONSUMPTION

ACHIEVE GREATER SUPPLY RELIABILITY
DRIVE INTELLIGENT PRODUCTION
DEFEND AGAINST CYBER ATTACKS
MOTOROLA SOLUTIONS
INDUSTRIAL INTERNET OF THINGS

CONTROL CENTER
- CONTROL CENTER APPLICATIONS
- FRONT END PROCESSOR GATEWAY
- MOBILE APPLICATIONS

NETWORK OF NETWORKS
- ASTRO® 25
- TETRA
- PRIVATE BROADBAND
- DIAL-UP MODEM
- PUBLIC 3G/4G
- ETHERNET
- FIBER

OPERATIONAL TECHNOLOGY
- M2M Modem
- SCADA RTU

SENSORS AND OTHER INTELLIGENT ELECTRONIC DEVICES

MOBILE APPLICATIONS

CONTROL CENTER

WAN
EMPOWER YOUR ELECTRICAL UTILITY TO MEET ESCALATING DEMANDS

A command center operator looks over CommandCentral Aware to monitor assets for alerts sent from the IRM1500 and data can be stored for trend analysis and historical system analysis.

A communication gateway interprets and converts data transmission to provide data in the correct size and bandwidth to the control system and servers from the field devices.

Land Mobile Radio Communications Network

The IACE 3600 sends an alert to a centralized control room based on sensors registering any physical breaches to a site such as door openings and movement.

An ACE3600 measures current flow from sensors on remote power lines and substations and sends periodic updates to a centralized control. In the event of a disruption an alert will be registered based on the precise location for a quick and accurate response.

REMOTE MONITORING & ALERTING WITH M2M OVER LMR COMMUNICATION NETWORK
EMPOWER YOUR ELECTRICAL UTILITY TO ENABLE EFFICIENT POWER DISTRIBUTION AUTOMATION

QUICKLY AND EASILY ISOLATE FAULTY SECTIONS ENSURING CONTINUOUS POWER
MINI DSM SCADA PROJECT

- Customer: Kenya Power and Lightening Company
- Electrical contractor El-Mor Israel
- Project scope: Pole top (150) and RMU (50) automation
- Deliverables: SF6 switches, Installations
- Motorola Deliverables: Design, 1 VHF Repeater, 200 RTUs, SCADA HMI
TYPICAL LBS CONFIGURATION

The requirements:
• To operate the Load Break Switch (LBS) Motor
• Advanced Fault detection

RTU
Radio
Local/Remote Sw.
Battery
Fault Detection Unit
Power Supply, Battery charger
Substation Screen
Feeder screen, one line diagram
LBS screen

Switch: Y501  RTU Id: 101
Sub-Region: N/WEST  Substation: HILL2
Feeder: Location: Inside All Saints Cathedral.

0.0 kV  0 A  0.00 Hz

RTU
Last update: 00:00
- Communication
- I/O module
- Power meter
- RTU off - no battery

Control cabinet
- Battery: 0.00 VDC
- C.B. ON
- 110 VAC
- Low battery
- Door open

Line Breaker Switch
- Last command
  - Closed
  - Remote
  - Open
  - Local
  - C.B. ON
  - Command fail

The legend:
- Normal status
- Fault
RTU status screen

<table>
<thead>
<tr>
<th>RTU Id</th>
<th>Poll</th>
<th>Comm.</th>
<th>Update</th>
<th>I/O</th>
<th>PM</th>
<th>AC</th>
<th>Batt</th>
<th>LBS Status</th>
<th>LBS Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>1001</td>
<td>Poll</td>
<td></td>
<td>00:00</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Closed</td>
<td>Control</td>
</tr>
<tr>
<td>1002</td>
<td>Poll</td>
<td></td>
<td>00:00</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Open</td>
<td>Control</td>
</tr>
<tr>
<td>1003</td>
<td>Poll</td>
<td></td>
<td>00:00</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Closed</td>
<td>Control</td>
</tr>
<tr>
<td>1004</td>
<td>Poll</td>
<td></td>
<td>00:00</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Closed</td>
<td>Control</td>
</tr>
<tr>
<td>1005</td>
<td>Poll</td>
<td></td>
<td>00:00</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Closed</td>
<td>Control</td>
</tr>
<tr>
<td>1006</td>
<td>Poll</td>
<td></td>
<td>00:00</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Closed</td>
<td>Control</td>
</tr>
<tr>
<td>1007</td>
<td>Poll</td>
<td></td>
<td>00:00</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Open</td>
<td>Control</td>
</tr>
<tr>
<td>1008</td>
<td>Poll</td>
<td></td>
<td>00:00</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Closed</td>
<td>Control</td>
</tr>
<tr>
<td>1009</td>
<td>Poll</td>
<td></td>
<td>00:00</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Closed</td>
<td>Control</td>
</tr>
<tr>
<td>1010</td>
<td>Poll</td>
<td></td>
<td>00:00</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Closed</td>
<td>Control</td>
</tr>
</tbody>
</table>
### SUPPORTED MEDIA’S

<table>
<thead>
<tr>
<th>*Analog Radio</th>
<th>Cellular</th>
<th>Satellite</th>
<th>Wired</th>
<th>Microwave</th>
<th>Data Radio</th>
</tr>
</thead>
<tbody>
<tr>
<td>DM4400</td>
<td></td>
<td></td>
<td>Leased line</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Fiber Optics</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* Two way analog is currently being supported by only the ACE3600
OPTIMIZE DATA FOR INCREASED EFFICIENCY

For organizations that need to be able to send a high volume of short data messages, ASTRO 25 Enhanced Data can increase inbound data efficiency up to 12 times and enable denser network traffic. This can be beneficial for GPS applications – tracking users at a higher cadence.

- Dynamically assign data channels
- Dedicate channels to data-only to preserve data capacity
- Support more GPS users at a higher cadence
WITH THE “GAIN” OF AN ADVANCED AUTOMATED GRID COMES SOME “PAIN”

40% INCREASE IN CYBER ATTACKS AGAINST THE ENERGY SECTOR¹

$10 BILLION IMPACT OF THE LARGEST BLACKOUT IN NE U.S. AND CANADA²

67% COMPANIES WITH ONE OR MORE SECURITY COMPROMISES CAUSING DISRUPTION²

78% LIKELY ATTACK ON SCADA OR ICS SYSTEMS IN THE NEXT 24 MONTHS³
Secure the Industrial IoT-Cyber Attack

83% of the organizations say cyber attacks are the one of their top 3 threats.

38% of organizations prepared for a cyber attack.
ARM YOUR IIoT SYSTEMS WITH PROACTIVE THREAT DETECTION, REAL-TIME CORRECTION & RESPONSE
PROTECT YOUR DAILY OPERATIONS FROM BEING COMPROMISED

100% INCREASE IN ATTACKS AGAINST INDUSTRIAL CONTROL SYSTEMS FROM 2013 TO 2014²

42.8 MILLION CYBERSECURITY ATTACKS IN 2014¹

85% OF BREACHES TAKE APPROX. 5 MONTHS TO DISCOVER³
Cyberterrorism is the use of the Internet to conduct violent acts that result in, or threaten, loss of life or significant bodily harm, in order to achieve political gains through intimidation.

Participating in a cyberattack affects the terror threat perception, even if it isn't done with a violent approach.
CYBER THREATS WITHIN ELECTRIC UTILITIES

- Insider Threats
- Malware & Spear Phishing Through Email
- Malware Targeting Data Stored on Servers
- Advanced Persistent Threats Residing on Computer Hard Drives

- Advanced Persistent Threats Through the SCADA System
- Denial of Service Blocking the Flow of Information Through System Operations

- System Operations Using SCADA Systems

- Insider Threats
WIDESPREAD VULNERABILITY REQUIRES SYSTEMATIC PROTECTION

NEW WAYS OF DOING BUSINESS DEMANDS SMARTER CYBERSECURITY: A BEST PRACTICE FRAMEWORK

CYBERSECURITY FRAMEWORK

IDENTIFY
ASSESS RISKS
Perform a thorough risk analysis
Uncover potential vulnerabilities

PROTECT
DEVELOP SAFEGUARDS
Develop policies and procedures
Implement appropriate access and auditing control

DETECT
MAKE TIMELY DISCOVERIES
Continuous monitoring 24x7x365
Enable auditing capabilities

RESPOND
TAKE ACTION
Establish a robust response plan
Correlate, analyze, triage and respond to detected events

RECOVER
RESTORE FUNCTIONALITY
Institute a recovery plan
Create improvements to prevent future attacks
INSULATE THE INTELLIGENT AT THE HEART OF YOUR OPERATIONS

THE CONTROL ROOM

UKR CC Video

WINDOWS HARDENING
Secure and lock down operating systems to minimize security threats and meet government standards (FISMA 2014)

ANTI-VIRUS SOFTWARE
Detect, prevent, and remove damaging code, such as worms, viruses, and Trojan horses on your computer.

APPLICATION CONTROL SOFTWARE
Block unauthorized applications and code from your servers, workstations and field devices by allowing only pre-identified and approved programs to run. The ACE3600 RTU and Gateway have application control mechanisms tested by McAfee Solidifier.

DEMILITARIZED ZONE (DMZ)
Tightly regular traffic entering servers with a combination of firewall and intrusion prevention systems. The DMZ eliminates common connection between the outside world and internal controlled zone.
EXTEND PROTECTION TO THE EDGE
ACE3600 REMOTE TERMINAL UNIT

ROLE-BASED ACCESS CONTROL
Assign specific roles and permissions to perform certain operations based on those roles, i.e., security admin could define roles and assign permission to each role.

FIREWALL
Permit or deny data transmission into your system or device based on rules and established criteria. All IP messages must pass through a firewall which examines each one and blocks those not meeting security criteria.

ACCESS CONTROL
Verify access to an RTU is legitimate from both other RTUs or system users with authentication.

APPLICATION CONTROL SOFTWARE
Block unauthorized applications from your components by allowing only pre-approved programs to run. The ACE3600 RTU and Gateway have application control mechanisms tested by McAfee Solidifier.

INTRUSION DETECTION SYSTEM
Automatically look for malicious activity or violates security policies. The ACE3600 will only allow legitimate traffic to enter and block malicious activity. Unauthorized activity is logged and can be reported to a designated control center.

ENCRYPTION
Data-at-Rest (DAR) protection ensures all data stored on devices or applications is encrypted with FIPS 140-2 validated AES 256 bit encryption significantly reducing the threat of lifting confidential data from compromised devices. Ensure secure data in transit with end to end encryption with AES 256 bit encryption.

AUDITING
Monitor any and all activity including suspicious activity or deviations from set security policy. Any attempt of unauthorized access to a secure ACE3600 RTU will be blocked and logged. The security log is encrypted and saved in FLASH memory to prevent malicious alteration and can be retrieved for forensic purposes after the event.

UNUSED PORT DEACTIVATION
The ACE3600 RTU enables unused ports to be disabled, reducing its vulnerability to unauthorized access.

TIME-WINDOW COMMANDS
Add additional layer of defense to limit the risk of replay attacks such as disgruntled employee with legitimate access. Timestamps are added to the command messages. The subsequent “action” must be received within a designated time and contain elements that match otherwise the action will be rejected.
High Level Security Architecture

Control Center
- Windows Hardening
- Unused Port Deactivation
- Anti-Virus Software
- Application Whitelisting
- Time-Window Commands
- Security Event Logging
- Secure IT Admin
- Access Control
  - Role-Based Access Control
  - Security Policy Enforcement

Operational Technology
- Secured ACE3600
- AES 256 End-to-End Encryption
- Service Access Architecture
- Demilitarized Zone
- Firewall
- WAN
INTERNET OF THINGS: LMR ADVANTAGES

**COVERAGE**
Without Compromise

Custom design meeting your requirements

**CAPACITY**
For All

Engineered for peak usage ensures information always gets through

**COST SAVINGS**
On a Large Scale

Predictable cost

**CAPABILITIES TO IMPROVE**
Situational Awareness

Purpose-built devices with data capabilities that augment voice and provides always available communications

**CONTROL**
For Security

High degree of control over system requirements, design, priorities, features and operations
PROTECT YOUR INDUSTRIAL
INTERNET OF THINGS ACE3600

- Authentication
- Intrusion Detection System
- Application Whitelisting
- Data at Rest Protection
  AES 256 Encryption
- Unused Port Deactivation
- TCP/IP Connection

Protect all points of entry, limit points of vulnerability and prevent attempts to compromise any part of your systems and data with these prove security methodologies.
INDUSTRIAL IoT IN ACTION
TAIWAN POWER COMPANY (TPC)
TAIPEI, TAIWAN

BACKGROUND

SUPPLY HIGH QUALITY & REASONABLE POWER TO MORE THAN 11.1 MILLION INDUSTRIAL, COMMERCIAL AND RESIDENTIAL CUSTOMERS.

CHALLENGE

NEED TO MINIMIZE THE IMPACT OF POWER LOSS DUE TO GROWING THREAT OF NATURAL DISASTERS

IMPLEMENT ELECTRIC DISTRIBUTION AUTOMATION FOR BETTER MONITORING AND CONTROL CAPABILITIES

CONNECTING TO EXISTING IED DNP3 PROTOCOL

DETECT FAULTS ON FEEDERS THAT CAUSE SWITCH PROBLEMS AND IDENTIFY PROBLEMS ON THE DISTRIBUTION NETWORK FOR IMMEDIATE RECTIFICATION

MONITOR THE VOLTAGE LEVEL AND SEND A MESSAGE REMOTELY WHEN THE LEVEL SLUMPS BELOW A CERTAIN SET POINT

COLLECT DATA AND GENERATE REPORTS THAT WILL HELP THE COMPANY TO RECTIFY, MANAGE AND PREVENT FAULTS AND PROBLEMS.

To read the entire case study click here
NORTHEASTERN US ELECTRIC UTILITY
INCREASE SERVICE AND DECREASE OUTAGES WITH SCADA

BACKGROUND

● IMPLEMENT A DISTRIBUTION AUTOMATION PROCESS

CHALLENGE

● HOW LEGACY 900 MHZ AND VHF WIRELESS SYSTEMS COULD BE LEVERAGED IN THE NEW SYSTEM?
● SEAMLESS ACCOMMODATE COMMUNICATION WITH IEDs FROM A VARIETY OF MANUFACTURERS USING NUMEROUS DATA PROTOCOLS

KEY BENEFITS

● QUICKER FAULT DETECTION AND ISOLATION
● AUTOMATED RESTORATION OF SERVICE
● MORE EFFICIENT PERSONNEL
● INCREASED CUSTOMER SATISFACTION

"Because a fully automated distribution system can take five to seven years to implement for a large utility, it’s important to have an extremely flexible network with the ability to adapt to advancements in protocols and technology as well as additional system requirements over the years."

To read the entire case study click here
MAKING THE GRID, SMARTER & Secured
IEC ISRAEL ELECTRIC COMPANY

BACKGROUND

- REQUIRED A NATION WIDE APPLICATION CONSISTING OF 170 SUBSTATIONS AND 2,500 RTUS
- COMMUNICATION OVER ANALOG VHF AND DATA ENABLED RADIOS
- REDUNDANT COMMUNICATION ON PUBLIC NETWORKS
- PROTOCOL MDLC
- SCADA FROM SIEMENS
- CYBER SECURED SYSTEM

CHALLENGE

- Country wide system required secured operation Migration process
- RF coverage limitation
- Number of units divided to several regions

KEY BENEFITS

- Fast detection of electric failure due to collected realtime information for the network
- Disconnect the failed region and Reroute the power by controlling the pole tops remotely
- Reduce power outage to minimum..
- Secured system
BACKGROUND
COUNTRYWIDE 13 REGIONS WITH SUB SYSTEMS
OPERATING ON ASTRO IV&D BASED COMMUNICATION
WITH PREVIOUSLY INSTALLED 460 RTUS

CHALLENGE
• Leverage the Countrywide P25 voice system to support also data communication for controlling the power network
• Migration of previous MOSCAD RTU with the ACE3600
• Supporting types of reclosers/breakers/capacitor bank from different manufacturers

KEY BENEFITS
• QUICKER FAULT DETECTION AND ISOLATION
• AUTOMATED RESTORATION OF SERVICE
• Use the existing P25 VOICE installation
KENYA POWER & LIGHTING COMPANY
NAIROBI, KENYA

BACKGROUND

KENYA POWER OWNS AND OPERATES MOST OF THE ELECTRICITY TRANSMISSIONS AND DISTRIBUTION SYSTEM IN THE COUNTRY TO OVER 4.8 MILLION PEOPLE

CHALLENGE

- Redundant control center
- Analog radio coverage around nairobi metropolitan

KEY BENEFITS

- QUICKER FAULT DETECTION AND ISOLATION
- AUTOMATED RESTORATION OF SERVICE
- MORE EFFICIENT PERSONNEL
- INCREASED CUSTOMER SATISFACTION
SUMMARY

• GSM/CELLULAR NETWORKS ARE ONLY AVAILABLE IN PLACES WHERE $$$ COULD BE GENERATED (POPULATED AREAS) OFTEN NOT AVAILABLE IN RURAL AREAS AND PLACES WHERE OUR GRIDS RUN

• Communication Systems Could be interconnected Regionally for collaboration just like a power grid is connected

• LMR SYSTEM FOR IOT SERVES AS A CLOSED CYBERSECURE ENVIRONMENT THAT IS HARD TO PENETRATE OR ATTACK

• LMR NETWORKS CAN COMBINE SECURE VOICE AND IOT DATA AND CAN BE SHARED ACROSS AGENCIES