

Standards to Promote Interoperability



U.S.-Africa Clean Energy
Standards Program



MOTOROLA SOLUTIONS

1st October-2018

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

MOTOROLA SOLUTIONS

ENSURING SAFER MORE PRODUCTIVE ELECTRICAL UTILITIES



1928
2018

YEARS



Agenda:

- 1. Mission Critical Communications for Electrical Utilities**
- 2. Mission Critical communications for IloT**
- 3. Sample Application**
- 4. IloT and Cyber Attack**

1st October-2018

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



- Group Calls
- Private Calls
- Telephony Interconnect
- Emergency Calls
- Emergency Alarm
- Messaging
- Embedded GPS
- Packet Data
- Authentication
- Bluetooth
- Encryption
- Direct Mode (Talk Around)

Enhanced Functionality & Performance



LIFELINE COMMUNICATION



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.

ASTRO 25 DATA APPLICATIONS AVAILABLE TODAY FROM MOTOROLA SOLUTIONS



LOCATION SERVICES

ASTRO 25 OUTDOOR GPS LOCATION

Track the location of your vehicles and personnel through either a dedicated GPS receiver or the integrated GPS in your APX radio.

ENHANCED GEO SELECT

Combine location, mapping and geofences to enable radios to



FLEET MANAGEMENT

OVER THE AIR SOFTWARE UPDATE

Update your entire fleet of radios in less than a week with no service disruption.

PROGRAMMING OVER P25 (POP25)

Reprogram radios over the air, eliminating the need to bring the



Digital Radio – Voice and Data

Regionally: Kenya , Ethiopia , Rwanda* chose to use the P25 Mission Critical Standard for Public Safety and for utility use



MESSAGING AND ALERTING

ASTRO 25 ADVANCED MESSAGING SOLUTIONS

Send and receive pre-programmed or free-form text messages to individuals or groups directly from two-way radios.

TALKGROUP TEXT MESSAGING

Broadcast detailed information via text to everyone in a talkgroup simultaneously.

MACH ALERT FIRE STATION AUTOMATION AND ALERTING

Alert multiple fire stations simultaneously and control elements in the firehouse such as closing doors and turning off stoves to improve response time, efficiency and safety.



MONITORING AND CONTROL

APX PERSONNEL ACCOUNTABILITY

Streamline on-scene roll calls, alert your team to changing incident situation and improve personnel safety.

SCADA & INDUSTRIAL IOT

From site security to fluid flows and electric grids, monitor and control remote sites and equipment with a variety of applications tailored to industry specific needs.





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

ALWAYS AVAILABLE



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



**LEVERAGE YOUR DATA
CAPABILITIES OF YOUR RADIO
NETWORK TO DEPLOY A
SECURE IOT/DMS**

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**



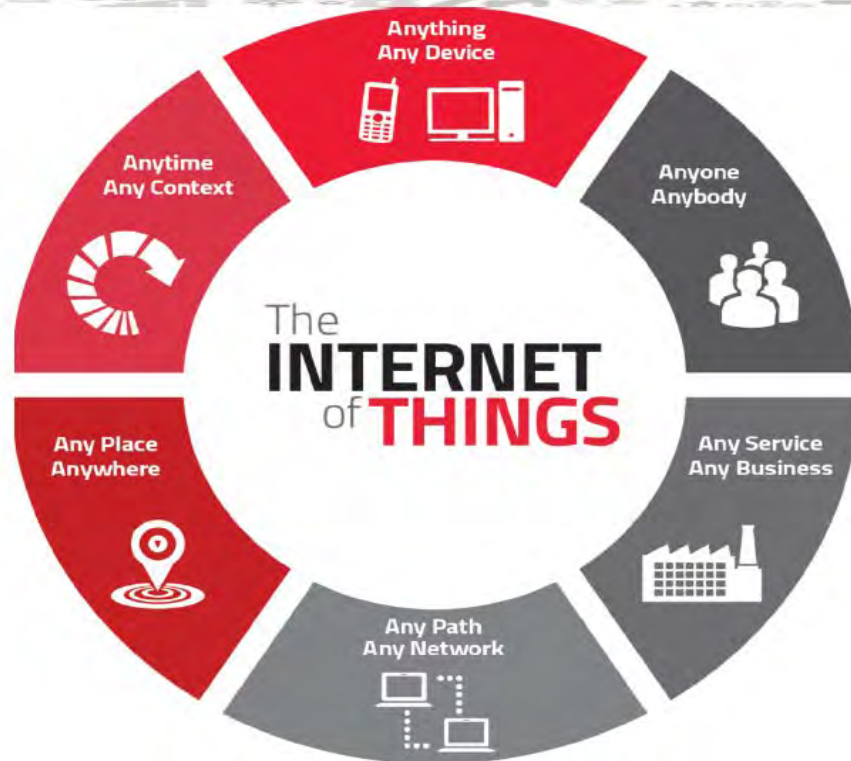
**ACHIEVE UNCOMPROMISING SAFETY
DRIVE INTELLIGENT PRODUCTION
WITH THE ASSURANCE OF ASSET SECURITY**



“ **TRANSFORM THE
ELECTRICAL UTILITY
ENTERPRISE BY
SEAMLESSLY
CONNECTING
WORKFLOWS,
PEOPLE AND
PROCESSES TO
REAL TIME
INFORMATION
ACROSS ANY
NETWORK**



What is IoT?





\$ 4 TRILLION INDUSTRY



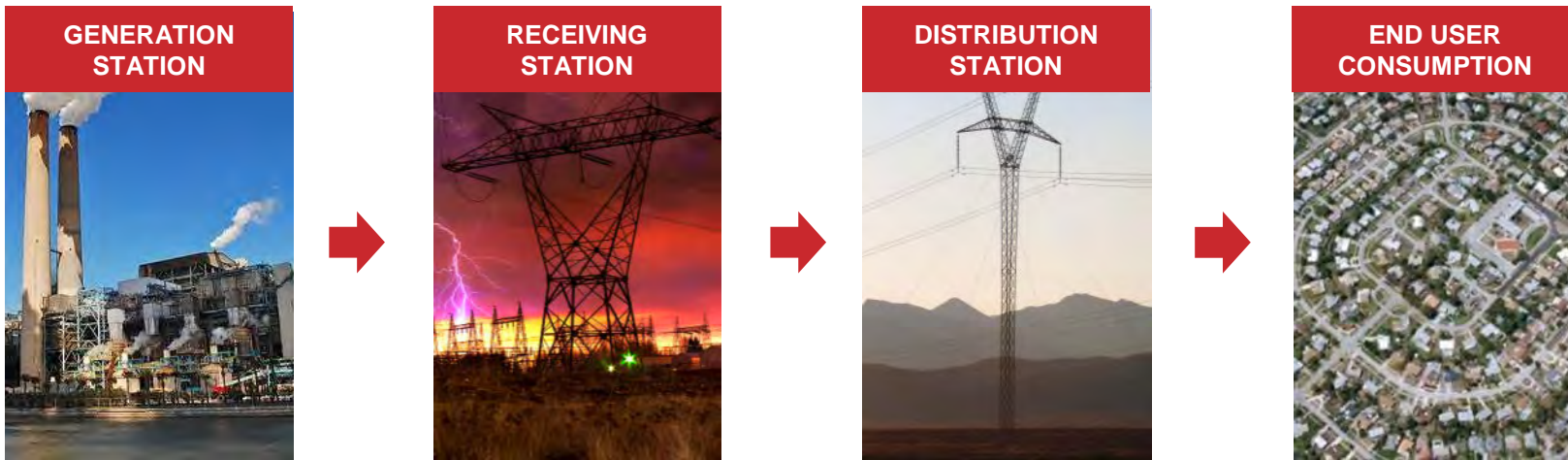
BY THE YEAR 2020, THERE WILL BE

50,000,000,000 connected devices,
creating and sharing

40,000,000,000,000 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

INDUSTRIAL INTERNET OF THINGS

TERM GLOSSARY



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

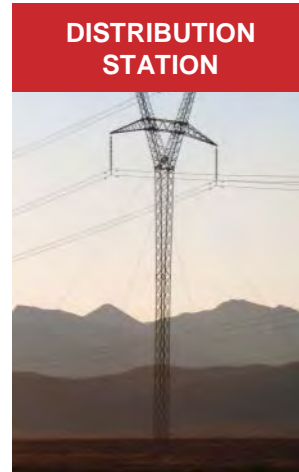
A combination of communication networks capable of working together to collect and communicate data across operations.

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



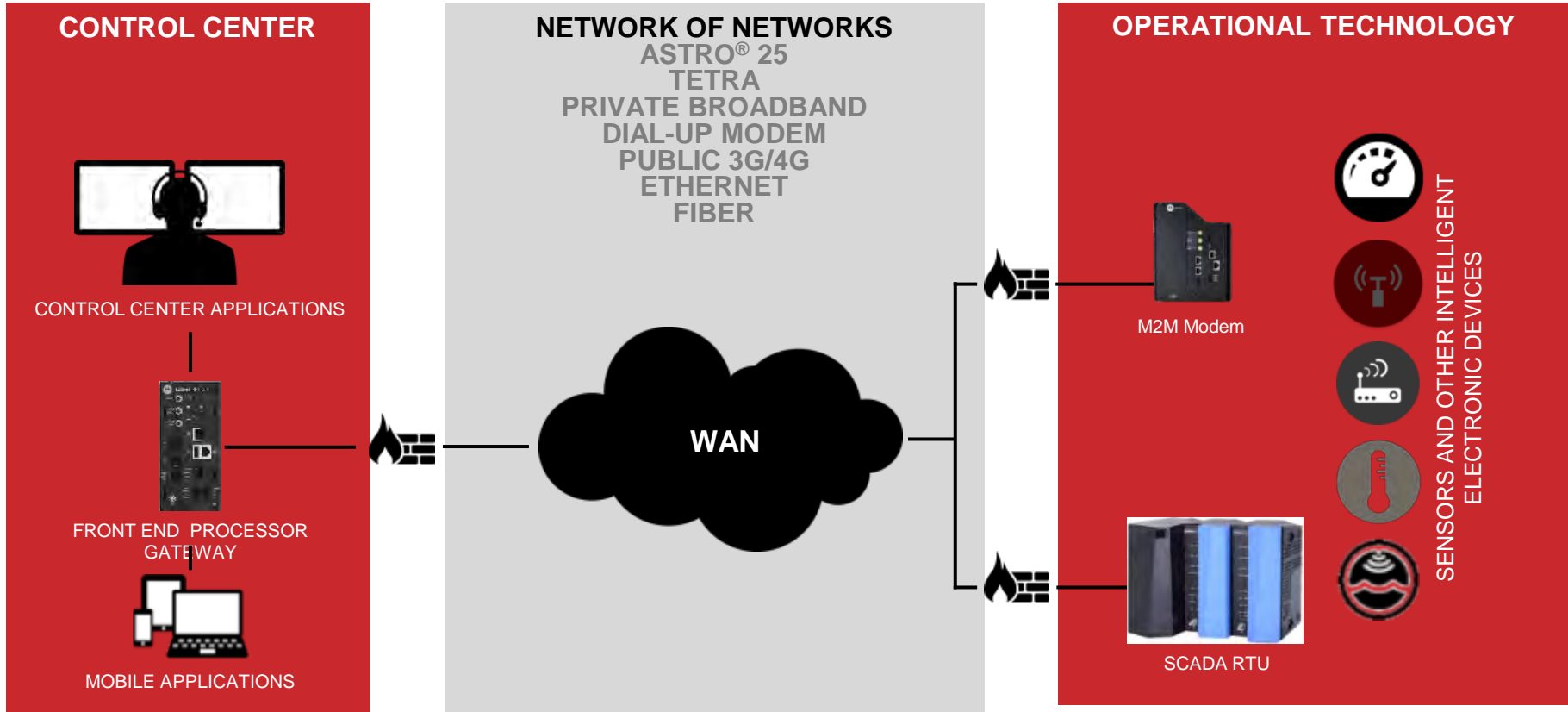
ACHIEVE GREATER SUPPLY RELIABILITY

DRIVE INTELLIGENT PRODUCTION

DEFEND AGAINST CYBER ATTACKS

MOTOROLA SOLUTIONS

INDUSTRIAL INTERNET OF THINGS



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



ACE360

SECURITY
ALARMS



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



ACE360

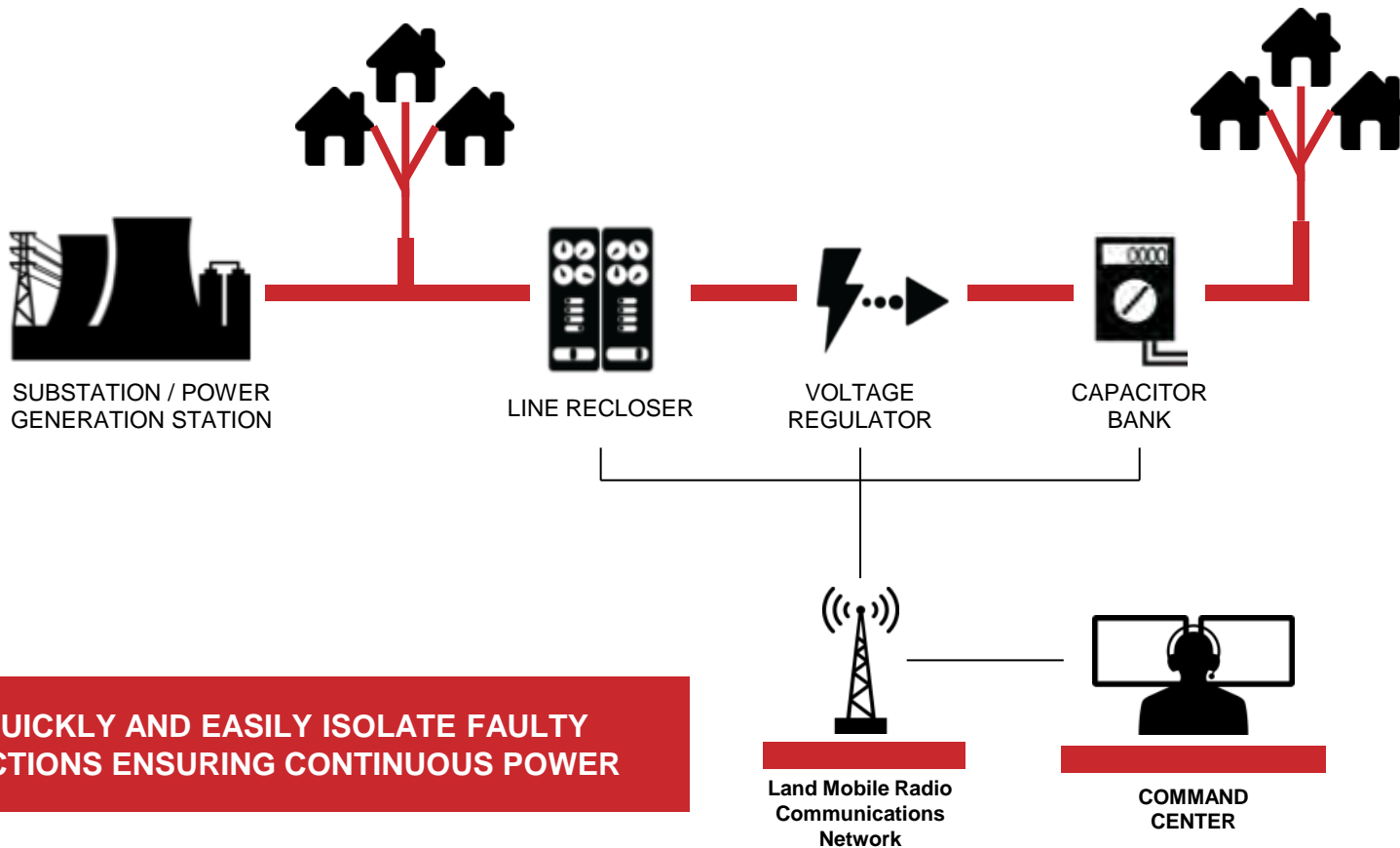
DATA
FLOW



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



MINI DSM SCADA PROJECT



- ❖ Customer: Kenya Power and Lightning 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.

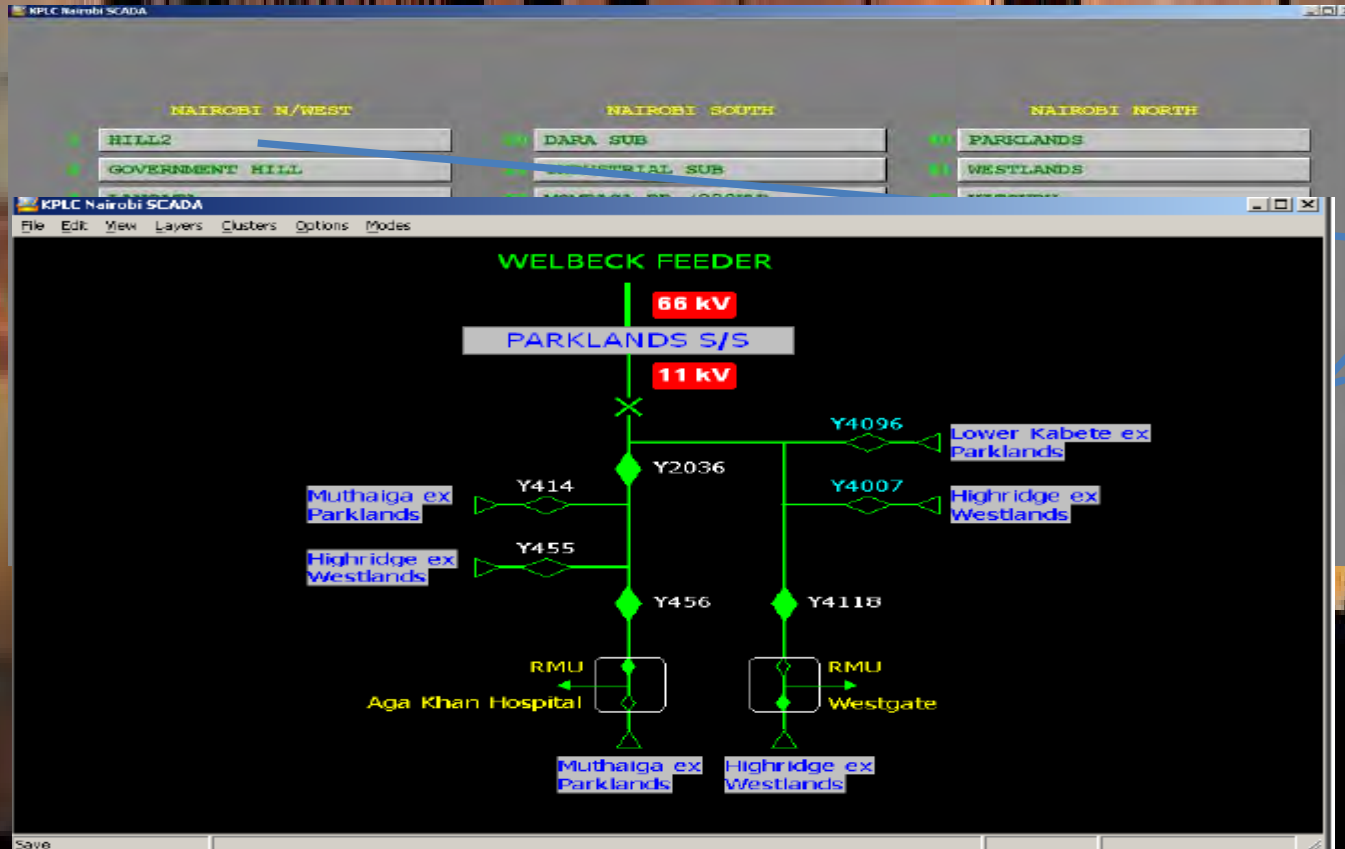
Battery

Fault Detection Unit

Power Supply , Battery charger



Substation Screen



Select Feeder

HIGHRIDGE

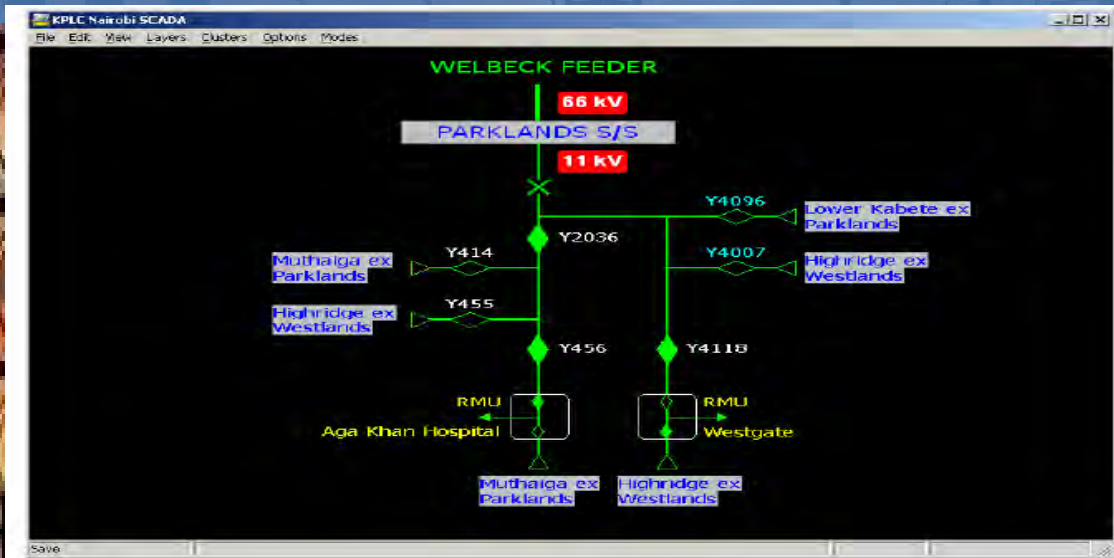
SARIT

PEPONI

WAIYAKI_WAY

Cancel

Feeder screen, one line diagram



Legend:

✕ - S/S exit circuit breaker

◆ - Closed LBS

◇ - Open LBS

Y2036 - manual LBS

Y4096 - Remotely Controlled LBS

Muthaiga ex Parklands
Connection to other feeder

LBS screen

KPLC Nairobi SCADA

Switch: Y501

RTU Id: 101

Sub-Region: N/WEST

Substation: HILL2

Feeder:

Location: Inside All Saints Cathedral.

10:50:57
03/01/2013

0.0 kV
0 A
0.00 Hz

R
S
T

0 A
0 A
0 A

Closed

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: CLOSE

- Closed
- Open
- C.B. ON
- Command fail
- Remote
- Local

The legend:

Normal status Fault

RTU status screen

RTU Id	Poll	Comm.	Update	I/O	PM	AC	Batt	LBS Status	LBS Control
1001	Poll		00:00					Closed	Control
1002	Poll		00:00					Open	Control
1003	Poll		00:00					Closed	Control
1004	Poll		00:00					Closed	Control
1005	Poll		00:00					Closed	Control
1006	Poll		00:00					Closed	Control
1007	Poll		00:00					Open	Control
1008	Poll		00:00					Closed	Control
1009	Poll		00:00					Closed	Control
1010	Poll		00:00					Closed	Control

SUPPORTED MEDIA'S



ASTRO® 25

APX6500
APX4000



Dimetra

MTM5200/5400



MOTOTRBO

DM4400 Connect +
DM4400

*Analog Radio	Cellular	Satellite	Wired	Microwave	Data Radio
DM4400			Leased line Fiber Optics		

* 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

ECOSYSTEM OF APPLICATIONS AND PARTNERS



THIRD PARTY DEVELOPER'S PROGRAM



Radio Control APIs

Remotely control portable radios and mobiles in the field.



Console APIs

Access ASTRO 25 console interface for dispatch and voice logging applications.



Network APIs

Receive, process and correlate events and alarms from ASTRO 25 network elements.



Data APIs

Send and receive short data messages to two-way radios over the ASTRO 25 IP data channel.

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 CANADA⁵



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 ORGANIZATION
PREPARED FOR A CYER
ATTACK**



**ARM YOUR IIoT
SYSTEMS WITH
PROACTIVE THREAT
DETECTION, REAL-
TIME CORRECTION
& RESPONSE**



PROTECT YOUR DAILY OPERATIONS FROM BEING COMPROMISED

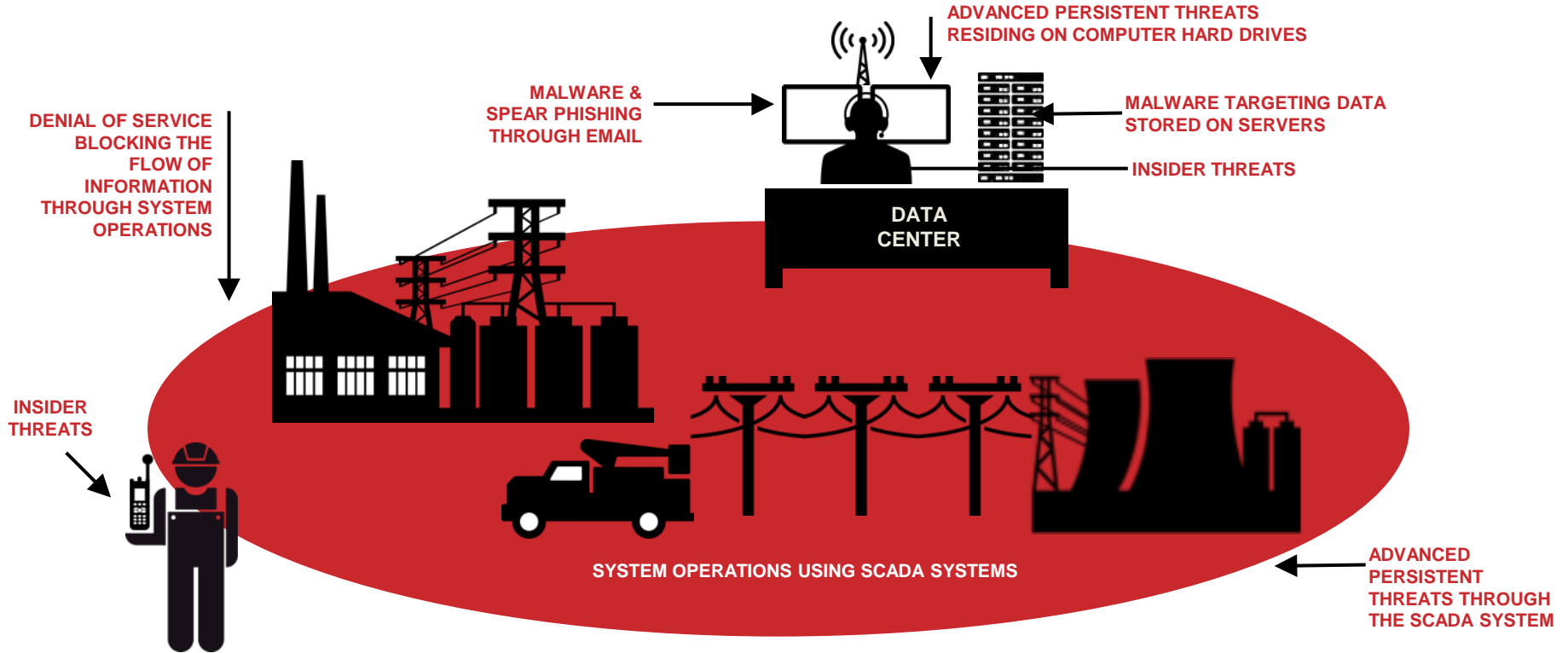




```
SendDlgItemMessage(hwnd, ID_RASER, CB_SELECTSTRING, -1, (LPARAM)adi[CurrTmNo].RasName);
if (!RasConnPresent) {
    EnableWindow(GetDlgItem(hwnd, ID_RASECSM), 0);
    EnableWindow(GetDlgItem(hwnd, ID_CHECKCONN), 0);
    EnableWindow(GetDlgItem(hwnd, ID_CUTRAS), 0);
    EnableWindow(GetDlgItem(hwnd, ID_CUTRAS), 0);
    IpREN=(RASENTRYNAME*)malloc((n=sizeof(RASENTRYNAME)))
}
if (!RasAPIPresent) {
    EnableWindow(GetDlgItem(hwnd, ID_CUTRAS), 0);
    pRasEnumEntries=0;
    for (b=0;b<gButtonNum) && !b:k++) b=b || !adiT[n].b;
    if (b) {
        CurrTmNo=k-1;SendMsgPage1(hwnd, CurrTmNo);
        SendDlgItemMessage(hwnd, ID_CBATN, CB_SETCURSEL, CurrTmNo, 0);
    }
}
switch (msg) {
case WM_CLOSE:
    EndDialog(hwnd, 0);
return 1;
}
int n,bufLen,bufit;
LPRASENTRYNAME lpREN;
free(lpREN);
if (RasAPIPresent)
    # (bufit>0) {
        if (strlen(ConnInUse)-->0) strcpy(ConnInUse,lpREN[0].szEntryName);
        free(lpREN);
        LPARAM lpREN;
        Tstn[n].h,"%i",adiArr[n].AITm.wHor;
        [n].m,"%i",adiArr[n].AITm.wMi;
        s,"%i",adiArr[n].AITm.wSec;
        case WM_INITDIALOG:
            for (n=0;n<gButtonNum;n++)
                adiT[n]=adiArr[n];
        BOOL GetErrDlgPg(HWND hwnd)
        int k; (LPARAM)lpREN[n].szEntryName);
        BOOL b=FALSE;
}

```

CYBER THREATS WITHIN ELECTRIC UTILITIES



WIDESPREAD VULNERABILITY REQUIRES SYSTEMATIC PROTECTION



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

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

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

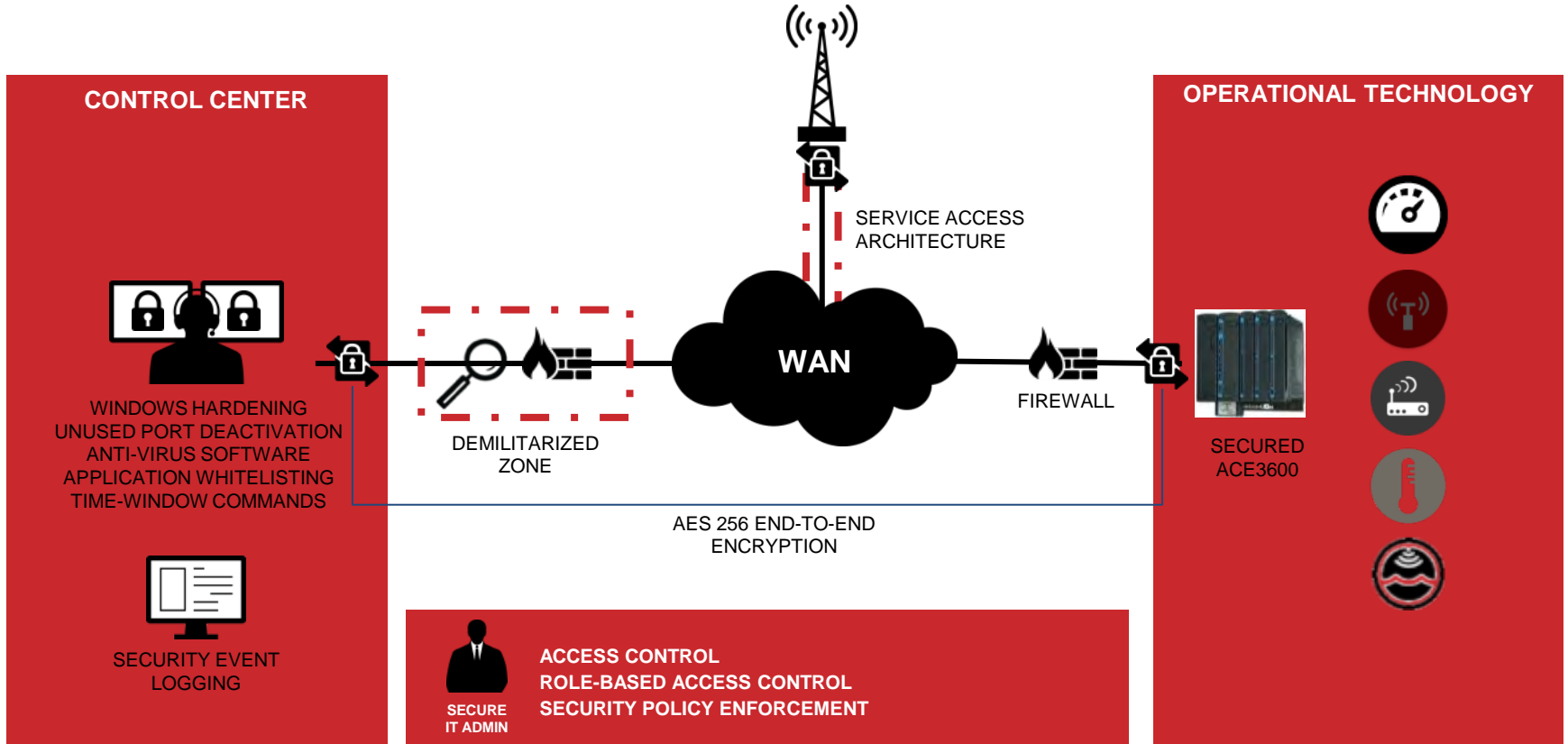
The ACE3600 RTU enables unused ports to be disabled, reducing its vulnerability to unauthorized access.



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



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**

**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**



**APPLICATION
WHITELISTING**

**DATA AT REST
PROTECTION
AES 256
ENCRYPTION**

**UNUSED PORT
DEACTIVATION**

**TCP / IP
CONNECTION**

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

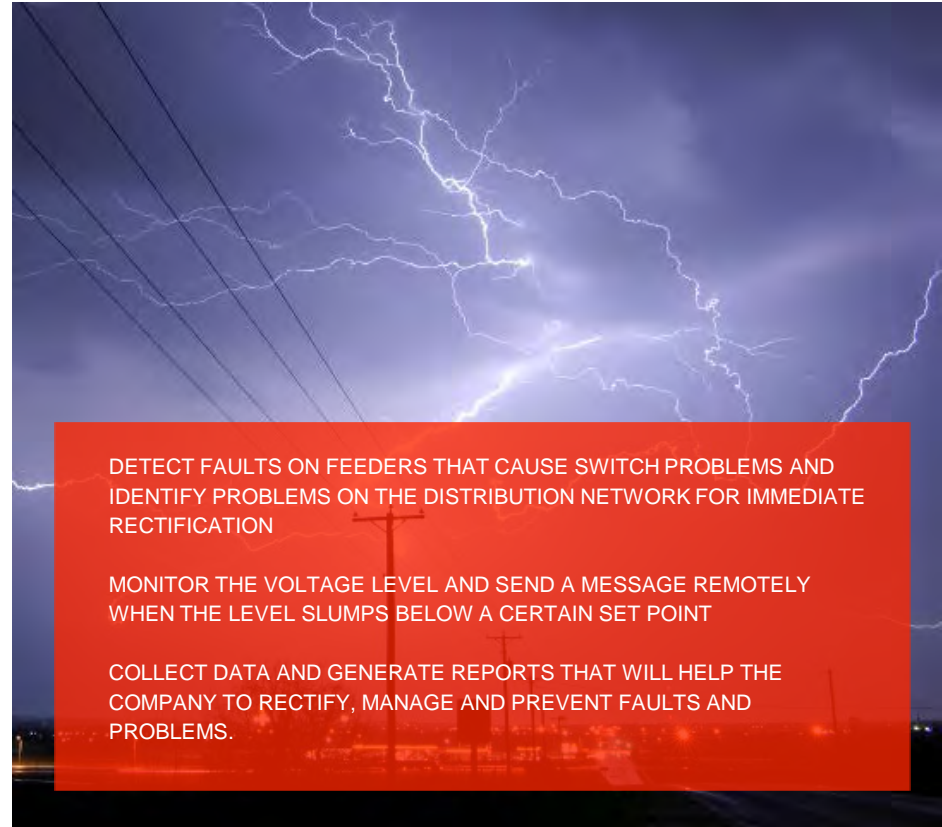
CONNECTING TO EXISTING IED DNP3 PROTOCOL

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

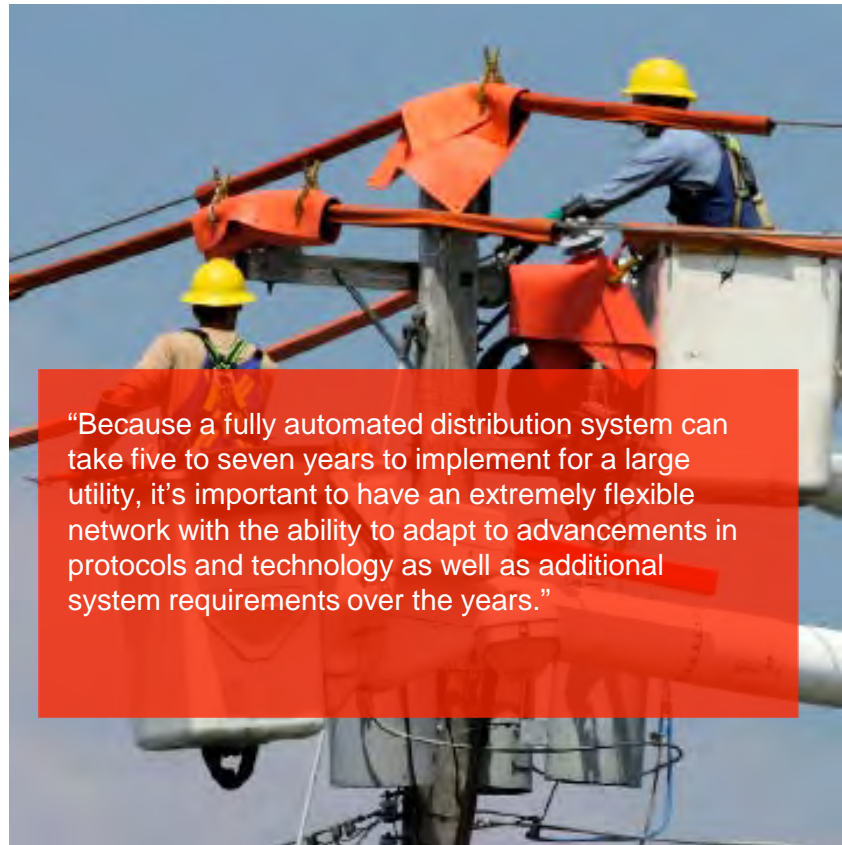
CHALLENGE

- 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

[To read the entire case study click here](#)



“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.”

MAKING THE GRID, SMARTER & Secured

IEC ISRAEL ELECTRIC COMPANY



Israel Electric

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



MURAKOZE

