Is Your SCADA Ready for the 21st Century?

Smart Water Summit

DOMINICK STORELI
TZVI MAGRIL
ASHLEY DIROU

September 7-9, 2016

MOTOROLA SOLUTIONS

MOTOROLA SOLUTIONS & SCADA

SUBJECT MATTER EXPERTS

- Over thirty years of experience in SCADA and other data communications for mission critical

MARKETS

- Water & Waste Water
- Electric Power Distribution
- Oil and Gas
- Environmental Monitoring & Early Warning
- Communication Systems
- Irrigation
- Transportation

MARKET SHARE

- Over 150,000 RTUs worldwide

DATA DRIVEN DECISIONS

(If you don’t see it, you can’t manage it)

SCADA @ GLANCE

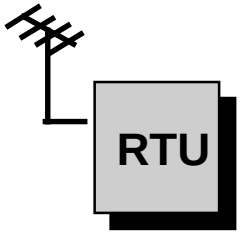
- SCADA is the IT backbone, based on Wide Area Network, for the monitoring and controls remote infrastructure
- SCADA provides Real Time, Accurate, Cyber Secured and Trusted information from the field, and guarantee Reliable Control
- SCADA must demonstrate high availability
- SCADA must dynamically and easily adapts to changes in the infrastructure
- SCADA must demonstrate high Longevity – 15-20 years
  - Evolutional upgrades vs. Rip & Replace

SCADA COMPONENTS

- SCADA Control Center
  - Central computer, alarm and event
  - Private or Cloud Based

- Data communications Network
  - Wide Area Network (WAN)
  - Wireless, Wire-Line, Optical;
  - Public and private networks

- Remote Terminal Units (RTU)
  - Combination of PLC and communication

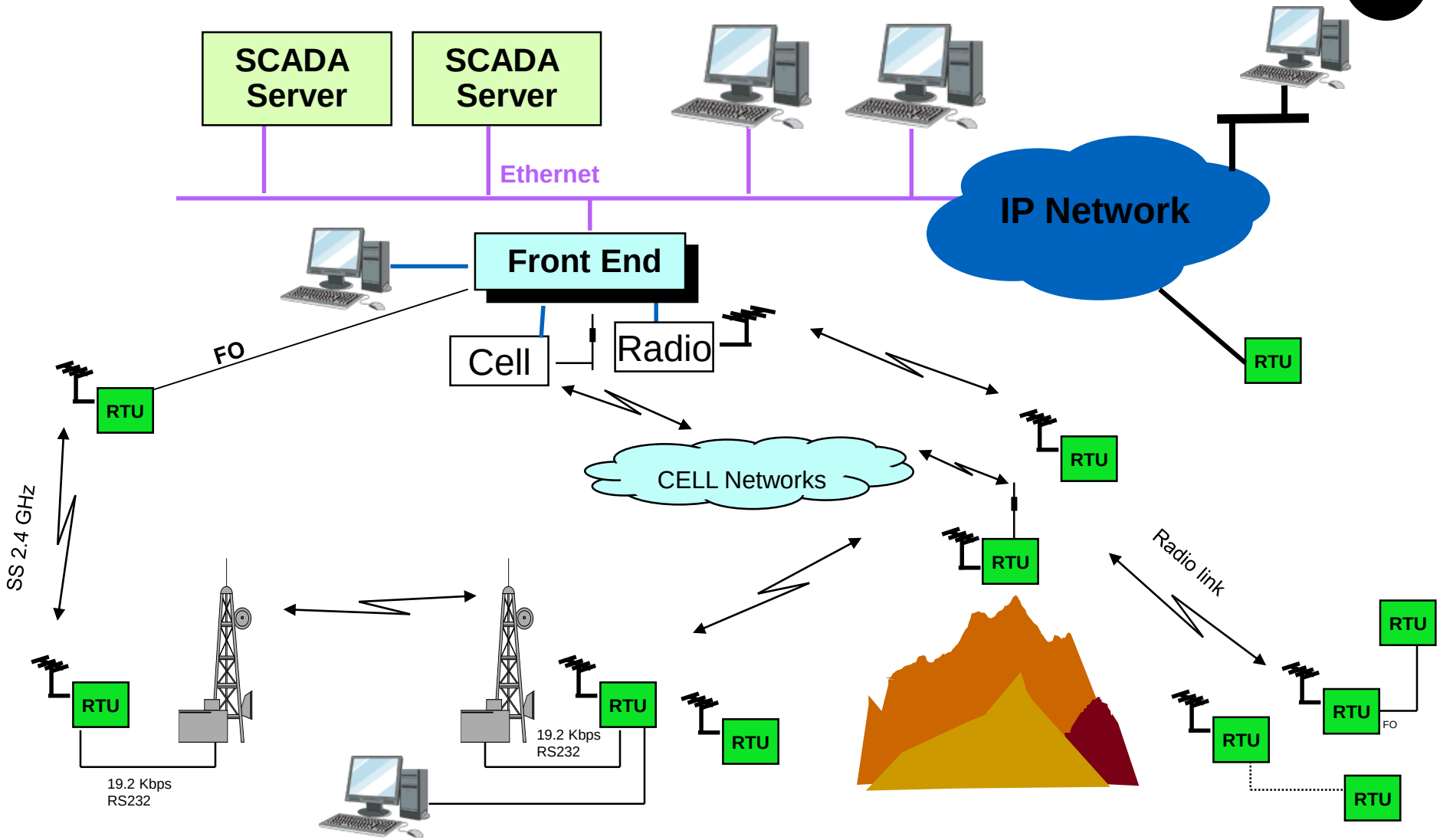


- Sensors and Control Device
  - Instrumentation
  - Smarts Sensors and Intelligent Devices

IS YOUR SCADA READY FOR THE 21ST CENTURY?

- Is your SCADA Ready for Hybrid of Network Technologies and Topologies?
  - Analog, Digital, Trunking, IP, Cellular, Broadband, Fiber optics, Line, PLCC, License, Unlicensed
  - Private and Public – Data usage, and availability of the cellular networks can be tricky
- Is you SCADA Cyber Secured?
- Is you RTU/PLC Ready to Integrate Smart Devices and Different Local Applications?
  - Smart Sensors, Smart Devices, Access Management, Surveillance
- Smart City Ready
  - GIS, Asset Management, CRM, ERP, AMR, Safe City
  - Integrate with IIoT technologies

HYBRID NETWORKS



CYBER SECURITY

SCADA Attacks on the Rise

- Most cyber attacks are not reported in public media
- Many attacks successful in achieving extortion payments
- Cyber attacks on Water/Wastewater facilities have increased substantially
- Attacks on Electric Utilities have increased 30 percent
- While no major cyber attacks on the US electric grid have been reported, Russia and China have “probed the electrical grid to find vulnerabilities to exploit if they needed to attack it,” said James Lewis, technology program director at the Center for Strategic & International Studies in Washington. Citing the National Security Agency, he said, “The risk is that the attack capabilities are spreading, and countries like Iran and North Korea, along with jihadists and anarchists, will eventually be able to attack.”

CYBER SECURITY (CONT.)

Growing Vulnerability of SCADA systems

- Networking – increased connectivity throughout the enterprise networks
- Insecure Remote Connections –some access links are vulnerable without encryption or authentication mechanisms
- Standardized Technologies – Microsoft's windows OS, third party SCADA SW
- Access to Information – design/maintenance documents and technical product manuals are readily available

How the Industry and Government Address the threat?

- Governmental actions and legislation
- SCADA is now handed by the IT departments, with knowledge of Cyber Security
- Wireless devices (e.g. cell modems) has encryption and authentication as standard feature
- Some SCADA protocols (e.g. MDLC, DNP3.0 Level 4) includes encryption
- Few vendors developed full fledged Cyber Security RTU/PLCs have

REQUIWIDESPREAD VULNERABILITY
RES 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

EXTEND PROTECTION TO THE EDGE
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.

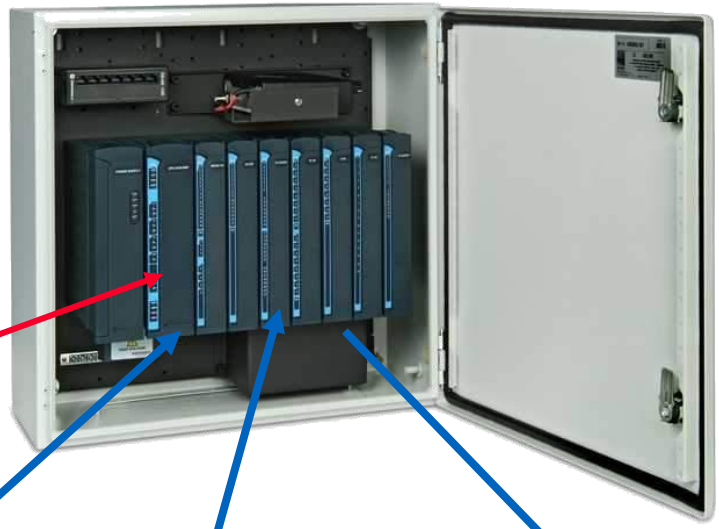
ENCRYPTION
Data-at-Rest (DAR) protection ensures all data stored on devices or applications is encrypted with FIPS 140-2 validated AES 256 bit encryption significantly reducing the threat of lifting confidential data from compromised devices. Ensure secure data in transit with end to end encryption with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

SITE MANAGER



Access Management
Site Surveillance

Smart Devices

Monitoring

Command

SMART & SAFE CITY INTEGRATED SOLUTIONS

Two-Way Radio

Bicycle
Rental solution

Motorola
RTVI

Cameras, Analytics
VMD

Mobile
Capabilities

Emergency
Sensor

IRRIG

WiFi

Air
& Water
quality Sensors

Inspectors
Locations

MotoCLOC CENTER

Integrated
Motorola
MotoBridge

THANK YOU