This webinar brought to you by the Relion® product family
Advanced protection and control IEDs from ABB

Relion. Thinking beyond the box.

Designed to seamlessly consolidate functions, Relion relays are smarter, more flexible and more adaptable. Easy to integrate and with an extensive function library, the Relion family of protection and control delivers advanced functionality and improved performance.

ABB Protective Relay School Webinar Series

Disclaimer

ABB is pleased to provide you with technical information regarding protective relays. The material included is not intended to be a complete presentation of all potential problems and solutions related to this topic. The content is generic and may not be applicable for circumstances or equipment at any specific facility. By participating in ABB's web-based Protective Relay School, you agree that ABB is providing this information to you on an informational basis only and makes no warranties, representations or guarantees as to the efficacy or commercial utility of the information for any specific application or purpose, and ABB is not responsible for any action taken in reliance on the information contained herein. ABB consultants and service representatives are available to study specific operations and make recommendations on improving safety, efficiency and profitability. Contact an ABB sales representative for further information.

ABB Protective Relay School webinar series

Wireless Communication Fundamentals
Adam Guglielmo
August 27, 2013

Power and productivity
for a better world™ ABB

Adam Guglielmo

Adam is a director of business development for ABB Wireless Communication Systems (formerly Tropos Networks) with a focus on Electric Utilities and Smart Grid.

He is based in Raleigh, NC and has over 14 years of experience in the telecommunications industry in product management, marketing, sales, and business development.

Before joining ABB, Adam spent more than seven years at Juniper Networks in a variety of roles. Before that, he was with Covad Communications and DirecTV Broadband.

Adam has a B.A. from Dartmouth College, a J.D. from the University of Colorado and is a member of the California State Bar.

Agenda

- Importance of the distribution area communication networks (DAN)
  - Common network infrastructure for multiple smart grid applications
  - Functional requirements for the DAN
- Key architectural choices for DAN
  - Public vs private networks
  - Licensed vs unlicensed spectrum
  - Mesh vs PTMP topologies
  - Standards based security vs closed and proprietary
- DAN architecture
  - System and network architecture and benefits

Smart grid evolution

	Early implementations	Current implementations
Applications	AMI	DA AMI, Demand response, …
Network	Single use Less reliable Narrowband High latency	Multi-use High reliability High bandwidth Low latency
Network Management	Element No traffic prioritization	FCAPS QoS

Wireless broadband enables smart grid applications

Distribution Automation
& Control

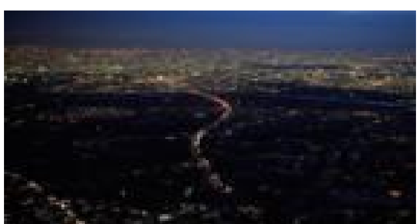
Automated
Metering

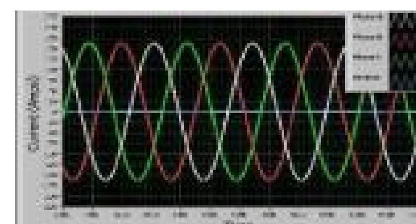
Renewables
Integration

Field Data
Applications

Demand
Response

Outage
Management

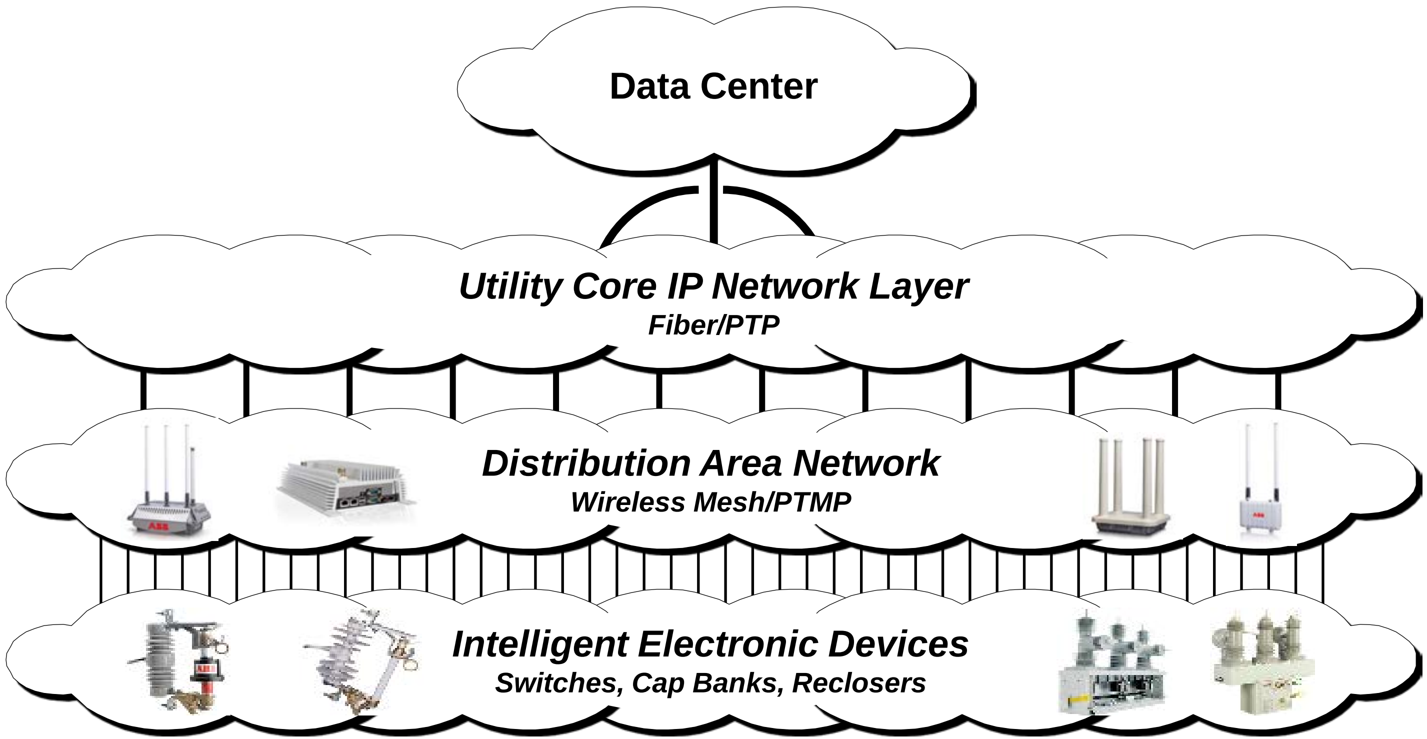




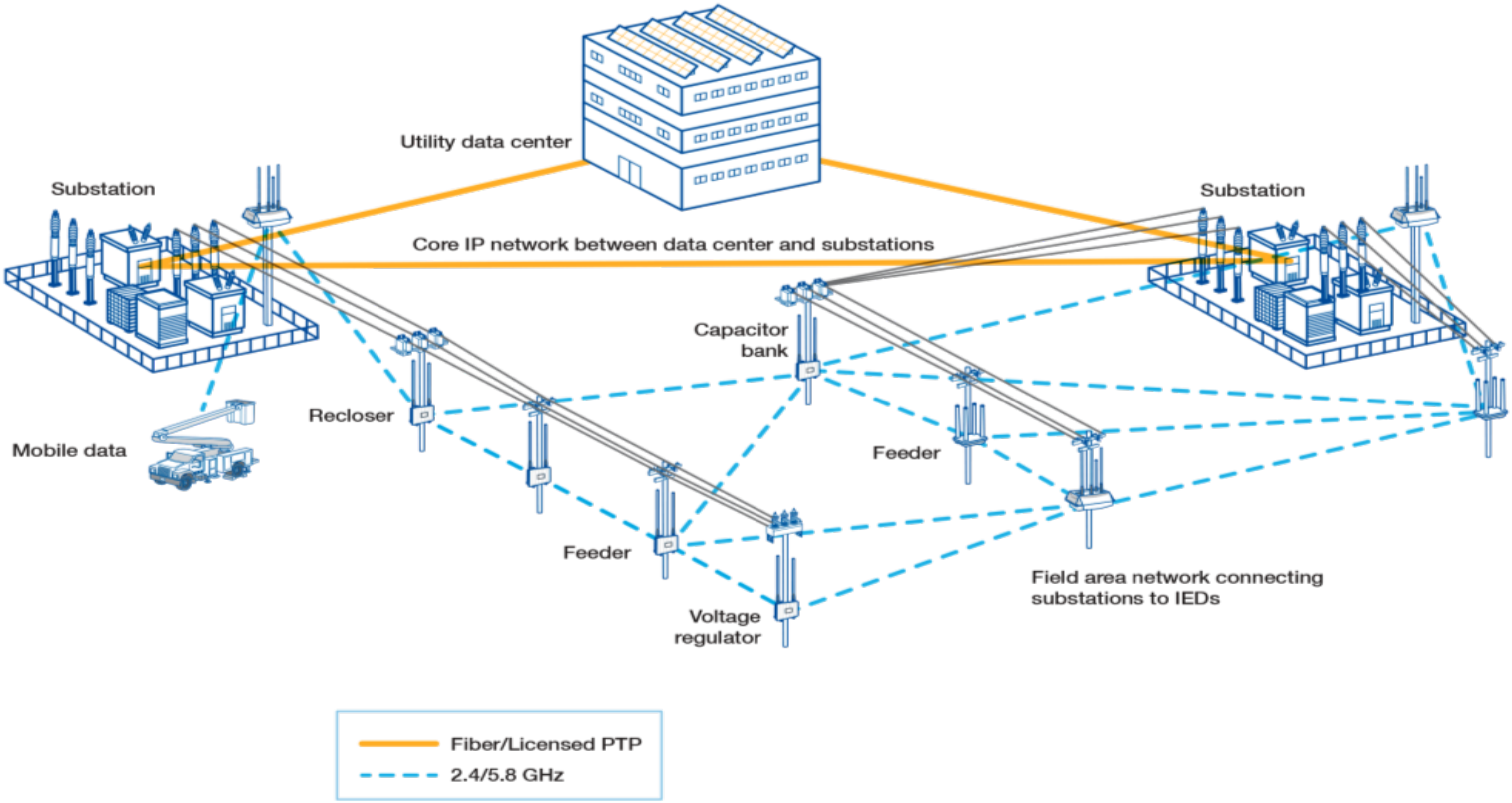
Power
Quality &
Planning

PHEV Integration

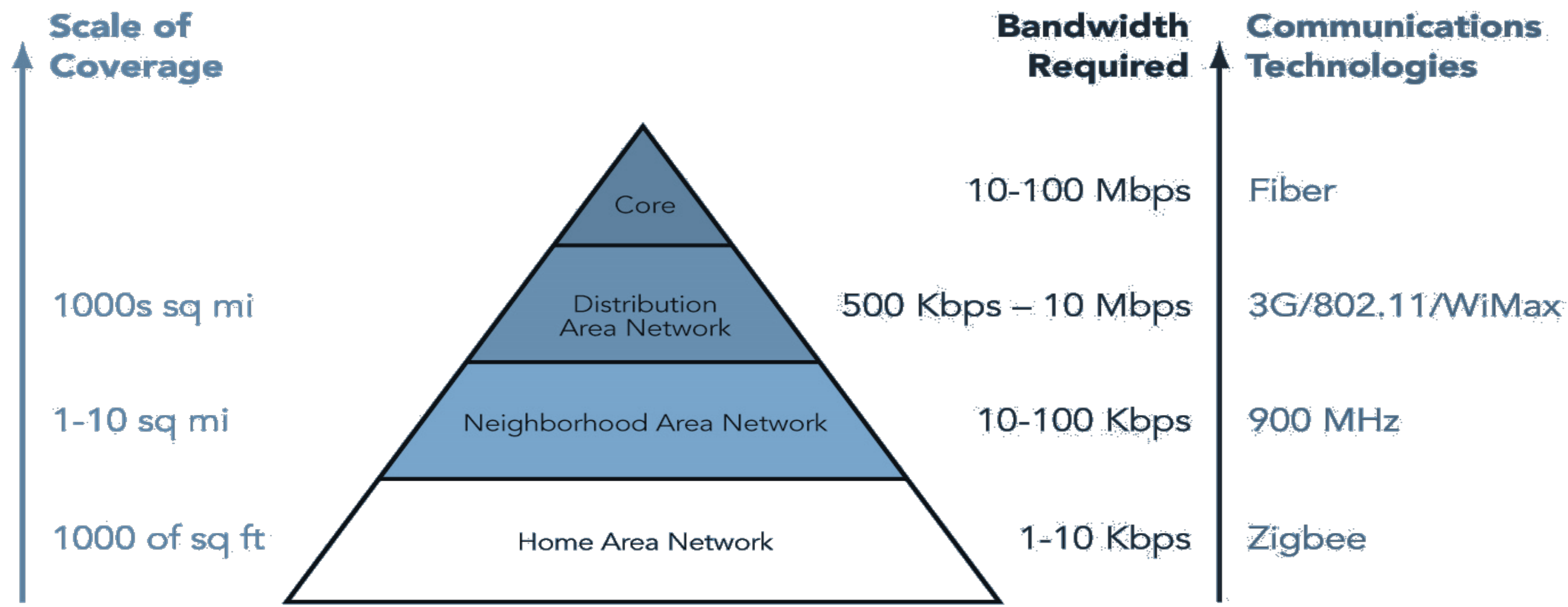
Broadband wireless distribution area networks
Fill gap between core network and field apparatus



DAN deployment example



Where do distribution area networks fit?



Applications drive performance requirements

Application	Latency	Bandwidth
Reclosers	10s msec	<56 kbps
Capacitor Bank	100s msec	<56 kbps
RTU	1000s msec	56 kbps
Motor Operated Disconnect	1000s msec	<56 kbps
Line Regulator	100s msec	<56 kbps
Advanced Metering	100s msec	56 kbps
IDR	100s msec	<56 kbps
Demand Mgmt	100s msec	<56 kbps
MWM Voice	100s msec	<56 kbps
MWM Data	100s msec	1000's kbps
Aggregate	10s msec	1000's kbps

Source: From IBM Presentation for the UTC on the Utility of the Future

- Other applications representing higher traffic include
  - Substation video
  - Plug in hybrid electric vehicle (PHEV) integration
  - Mobile geographic information systems (GIS)
  - Mobile workforce
  - and more in the future

Key architectural choices

- Public carrier networks or utility-owned private networks
- Licensed or unlicensed spectrum
- Point-to-multipoint (PTMP) or mesh
- Standards based security or closed/proprietary

Public or private networks?

Comparison of public and private networks

	Public	Private
Availability	Moderate-high availability	Can be designed to be very high availability (“five nines”)
Survivability	OK for non-critical data transport, inadequate for mission-critical apps	Highly survivable architectures and technology options
Coverage	Limited coverage in rural/lightly-populated areas	Can be engineered to very high levels, but requires mix of technologies
Latency	100-1000 ms	10-100 ms
Security	Adequate	Highly secure options exist
Life cycle	Largely outside utility control	Controlled by utility
Cost	Primarily OPEX	Primarily CAPEX

Private vs. public networks
Conclusions

- Economics depend on topography and device density
  - Broadband private networks cost-prohibitive in rural/low device density areas, use public network or narrowband private PTMP
  - Broadband private nets cost-effective in urban and suburban areas
- Networks that support mission-critical applications, require stringent performance or run multiple applications should use private networks
- Utilities that prefer upfront capital expenditure should deploy private, those preferring ongoing operational expense should use public
- Utilities that want control should deploy private networks
- Utilities looking to quickly fix a point problem should use public, those deploying a long-term grid modernization solution should use private
- Utilities with diverse service territories will need private/public hybrid
  - Private networks in urban/suburban areas
  - Public for fill-in coverage where private networks not economical

Licensed or unlicensed spectrum?

Private network spectrum options
Licensed vs. unlicensed comparison

	Licensed	Unlicensed
Licensing cost	High	None
Unit cost	High	Low
Spectrum quantity	Typically 10 kHz to a few MHz	170+ MHz, more in some countries
Spectrum availability	No global regime	Near-global availability for 2.4 GHz and 5 GHz
RF propagation	Depends on spectrum	Good
Throughput	Typically <1 Mbps	10 Mbps – 100+ Mbps
Interference concerns	Low	Low with cognitive radios
Security	Must be designed into system	Must be designed into system

Licensed or unlicensed – summary

- Licensed spectrum has some benefits, but
  - Has limited availability and only in small narrowband chunks
  - Very expensive to acquire
- Reality is
  - Unlicensed can be as/more secure, reliable, and much higher performance than licensed spectrum options

Cognitive radios and specialized hardware deliver reliable unlicensed spectrum operation

- Mitigate interference caused by other networks and devices
  - Redundant mesh with high path diversity
  - Distributed auto-channel and band algorithm
  - Dynamic transmit power and data rate control
  - Precision radio filters eliminate out-of-band interference
  - Maximal Ratio Combining (MRC) receivers (802.11n)
- Reduces interference suffered by other networks
  - Listen-before-talk protocol (802.11 CSMA/CA)
  - Superior receive sensitivity – won't unintentionally transmit over weaker neighbors
  - Dynamic Frequency Selection (DFS) avoids interfering with radar systems
  - Auto-channel and dynamic power/data rate control algorithms

Mesh or PTMP?

Mesh and PTMP architectures

- PTMP (point-to-multipoint) is a hub-and-spoke wireless topology
  - Common use cases
    - Capacity injection for a wide-area mesh
    - Connectivity to remote endpoints
    - Backhaul for remote substations
- Mesh is a self-organizing, self-healing architecture with routing path diversity and no single point of failure
  - Typically uses unlicensed spectrum
  - Examples include Zigbee mesh, AMI meter mesh, broadband mesh

Mesh superior to competitive wireless technologies

	SCADA Radio	Broadband PTMP	Broadband Mesh
Reliability	◑	◑	●
Bandwidth	◔	◕	◕
Latency	◕	◕	◕
QoS	○	◕	●
Coverage	●	◑	◕
Mobility	○	◔	◕
Security	◑	◕	◕
Manageability	○	◕	●
Future Proof	◔	◕	●
Standards-based	○	◕	●
Ease of deployment	◑	◔	◕

Poor ○ ⟷ ● **Best**

PTMP + mesh: 2+2=5

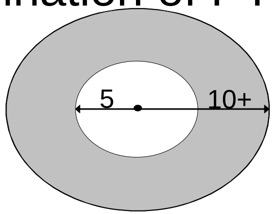
- PTMP and mesh are complementary technologies for the DAN
  - PTMP is very cost-effective for suburban and rural deployments and for mesh capacity injection in denser areas
  - Mesh is well-suited for urban areas providing resilience and higher capacity
- Optimal combination of mesh and PTMP leverages the strengths of both
  - Mesh extends coverage range of PTMP and improves reliability
  - Architectural resilience through mesh failover capabilities
  - Combined deployment achieves
    - Economics optimized for mix of urban/suburban/rural areas
    - Meets requirements for multiple DAN applications

Blending mesh and PTMP

Mesh + PTMP

Expand PTMP Cell Radius With Combination of PTMP + Mesh

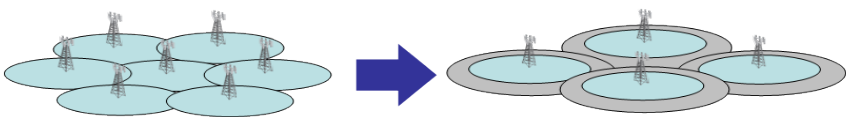
Reduce # of Towers



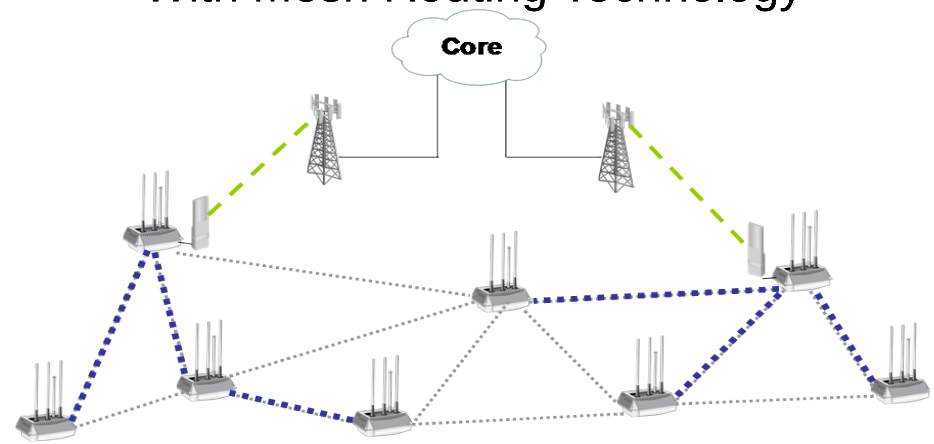
5 mile radius → 10+ mi radius

78.5 sq miles → 300 to 1,000+ sq miles

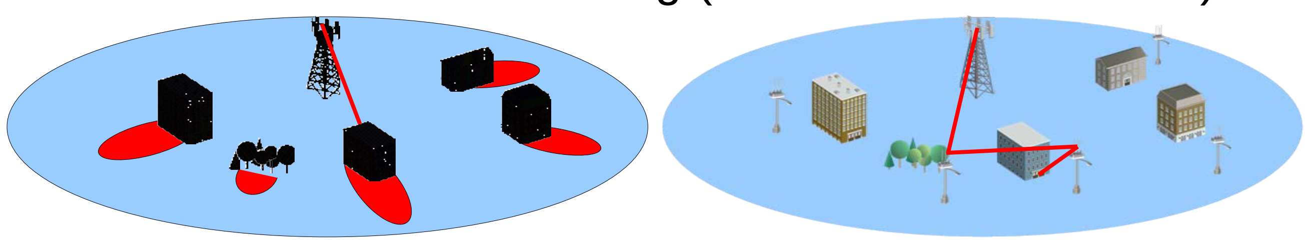
3 to 10 x coverage per tower



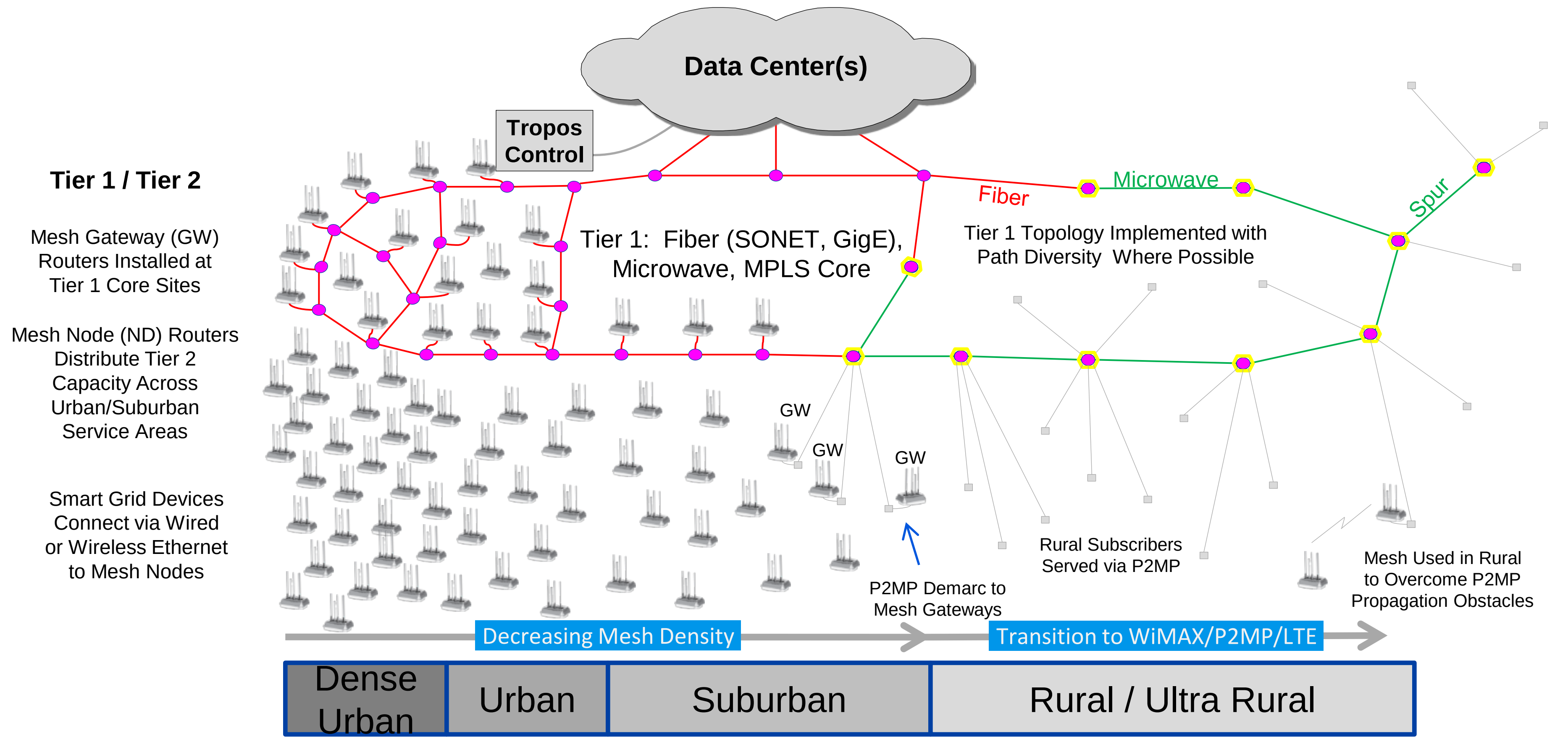
Increase System Availability (>99.99%) With Mesh Routing Technology



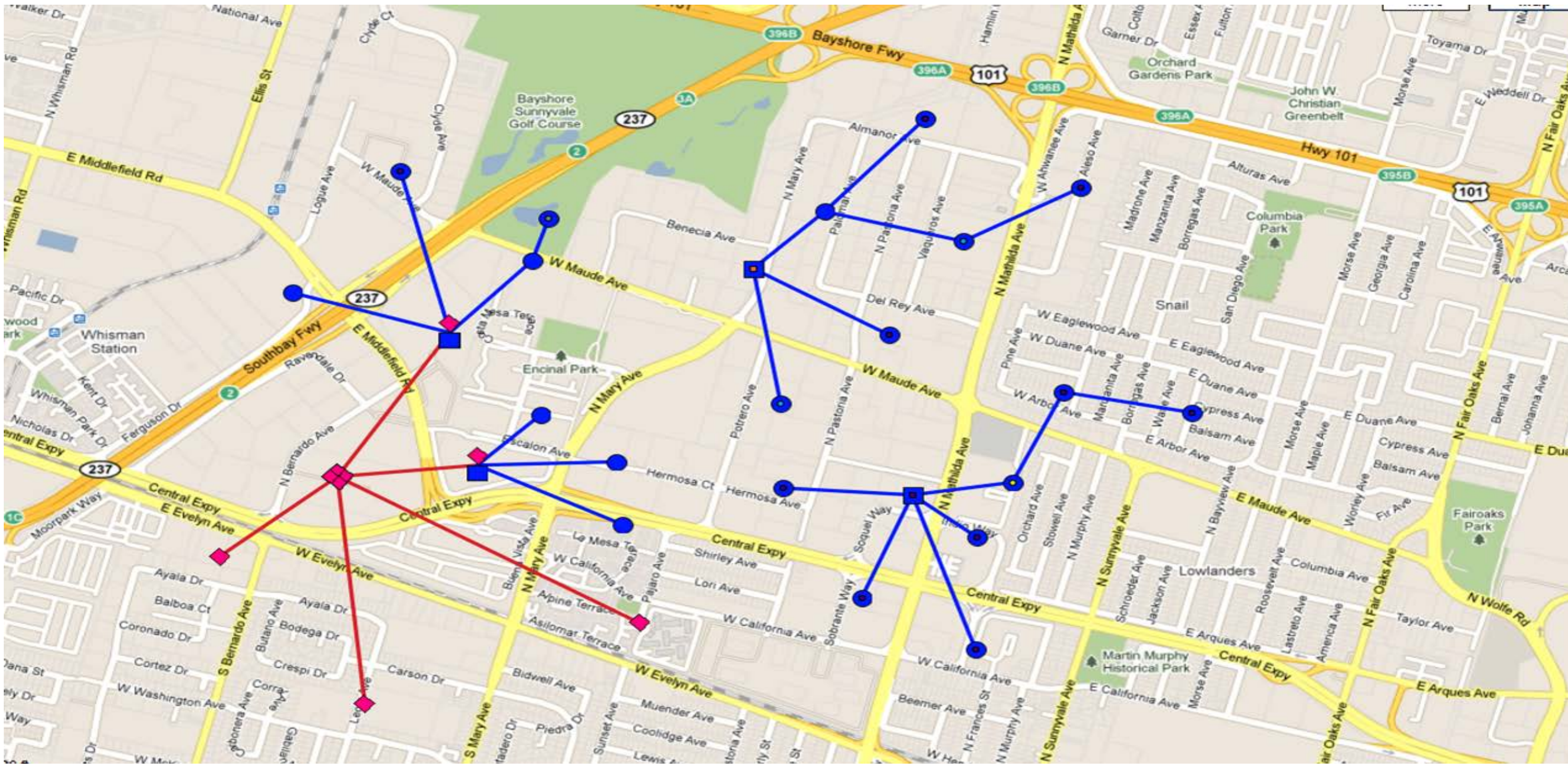
Eliminate PTMP Shadowing (route around obstacles)



Optimal technology mix



Unified visibility and management



Standards-based security vs. closed and proprietary

The smart grid brings increased fear of cyber attacks

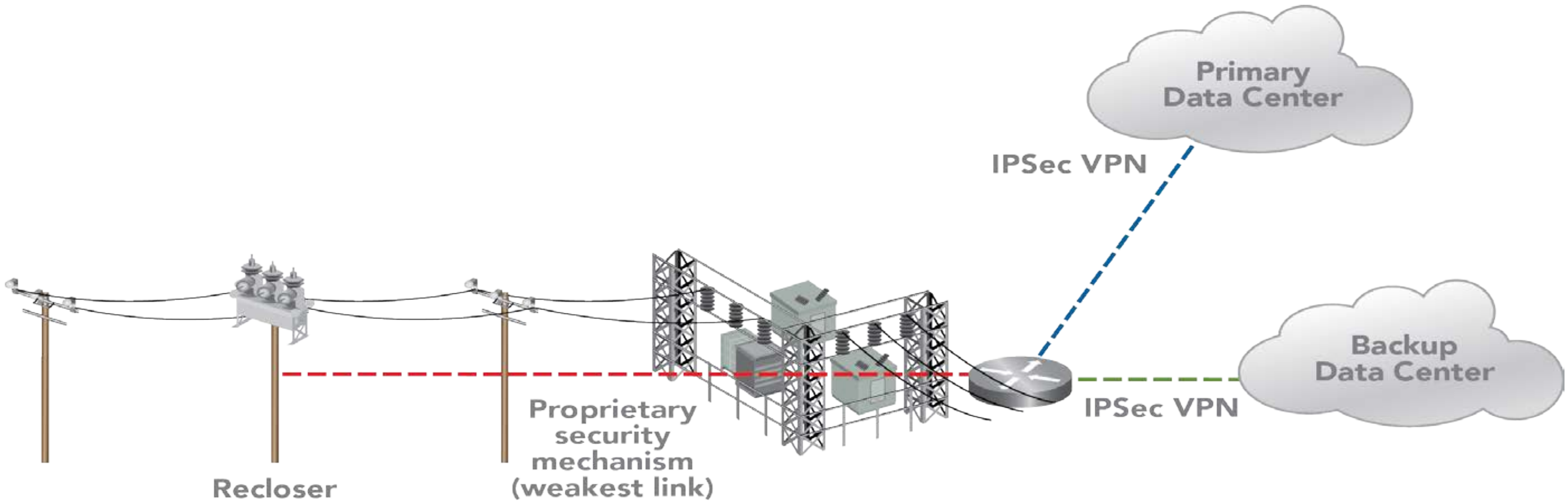
- The smart grid promises a fully-automated power delivery network with a two-way flow of information
- Utility systems have traditionally been physically-isolated, closed and proprietary
- To facilitate two-way information flow, utility systems are evolving toward integrated, networked, open IP-based architectures extended to distribution system assets
- With this increased functionality and integration, fear of cyber attacks is increased

Functional requirements for field network security
Multi-layer enterprise network security model meets these needs

- Network access control
- Network resource and remote endpoint protection
- User and device identification and authentication
- Secure end-to-end data transmission
- Traffic segmentation and prioritization across applications
- Secure network management
- Audit and accountability
- Availability and performance

Traditional point product solutions

Lack ability to extend standard, secure communications from data center to distribution automation endpoints



- Lack of access control mechanisms
- Lack of firewalls for endpoint and network protection
- Lack of user and device identification and authentication

Bringing enterprise class security to smart grid distribution area networks

- For more than a decade, enterprises have faced the same challenges that utilities now face with smart grid distribution area networks
- Enterprises rely on multi-layer, multi-application security models for defense-in-depth network security
- Standards-based approaches that have gone through peer reviews and have been time tested are better suited for a converging IP-based smart grids
- Standards and tools such as 802.1x, IPsec, 802.1Q VLANs, 802.1p QoS, and firewalls have successfully defended enterprises against a wide variety of cyber-attacks

Multi-layer security

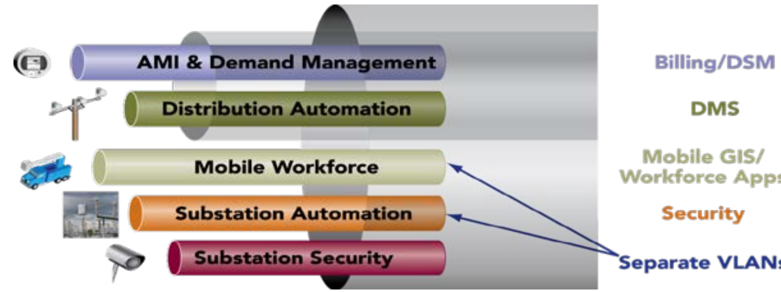
NERC CIP

FIPS

Layer	Security measures
Application	HTTPS, SNMPv3, XML/SSL
Transport	SSL/TLS
Network	IPSec, Firewall, IP ACLs
Link	802.1x access control, 802.11i authentication, AES encryption, MAC ACLs and whitelists/ blacklists, DoS detection and mitigation
Physical	Hardened outdoor enclosure, tamper-detection, encrypted file system, hardware authentication, protection of critical security parameters

Multi-application security

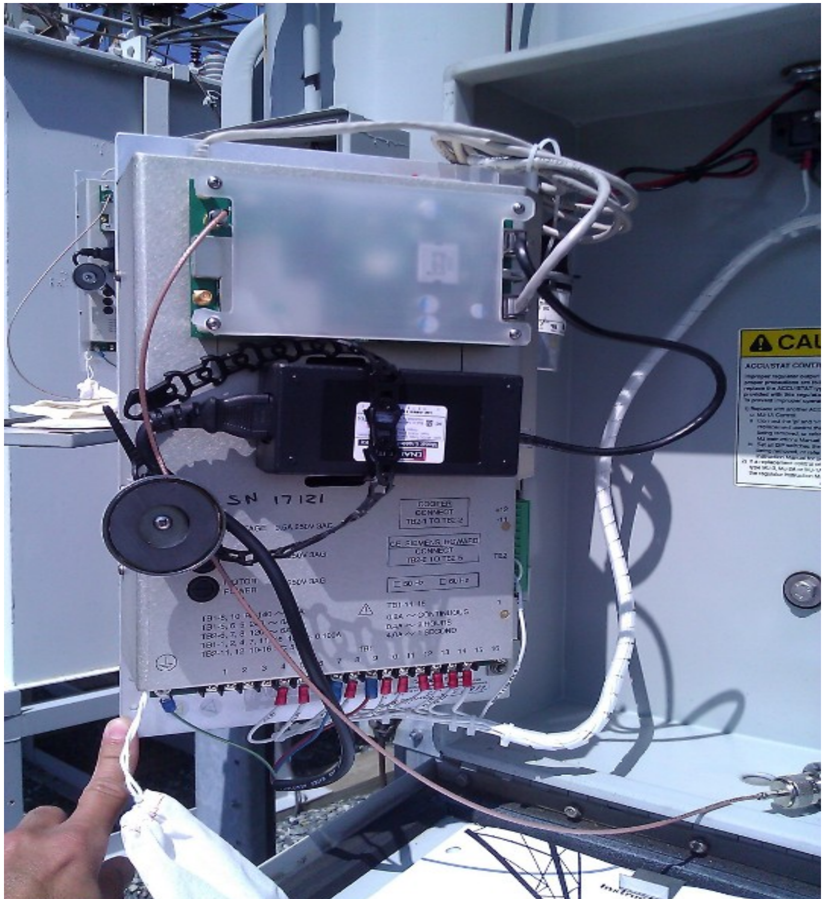
- Differentiated services over common wireless infrastructure
- Security and QoS policies per-VLAN using 802.1Q and 802.1p
- Traffic classification, prioritization, and segmentation
- Extends enterprise IT framework and policies into distribution system



DA	PQ Sensors	IT	AMI	Mobile Ops	Surveillance
SSID: DA	SSID: PwrQual	SSID: UtilIT	SSID: AMI	SSID: UtilOps1	SSID: Detect
Non Broadcast	Non Broadcast	Broadcast	Non Broadcast	Broadcast	Non Broadcast
802.1x	WPA	802.1x	802.1x	802.1x	802.1x
1 Mbps	500 Kbps	1 Mbps	256 Kbps	1 Mbps	2 Mbps
Priority 1	Priority 2	Priority 2	Priority 3	Priority 2	Priority 1

Implementation examples

East coast utility
Substation automation with integrated communications



- Starting a program to automate substations with SCADA (specifically voltage regulators)
- Communication requirements
  - Access to controls without running cables
  - Avoid drilling out control cabinets
  - Access to controls from anywhere within the substation
  - Support for proper cybersecurity standards

Wireless voltage regulator control

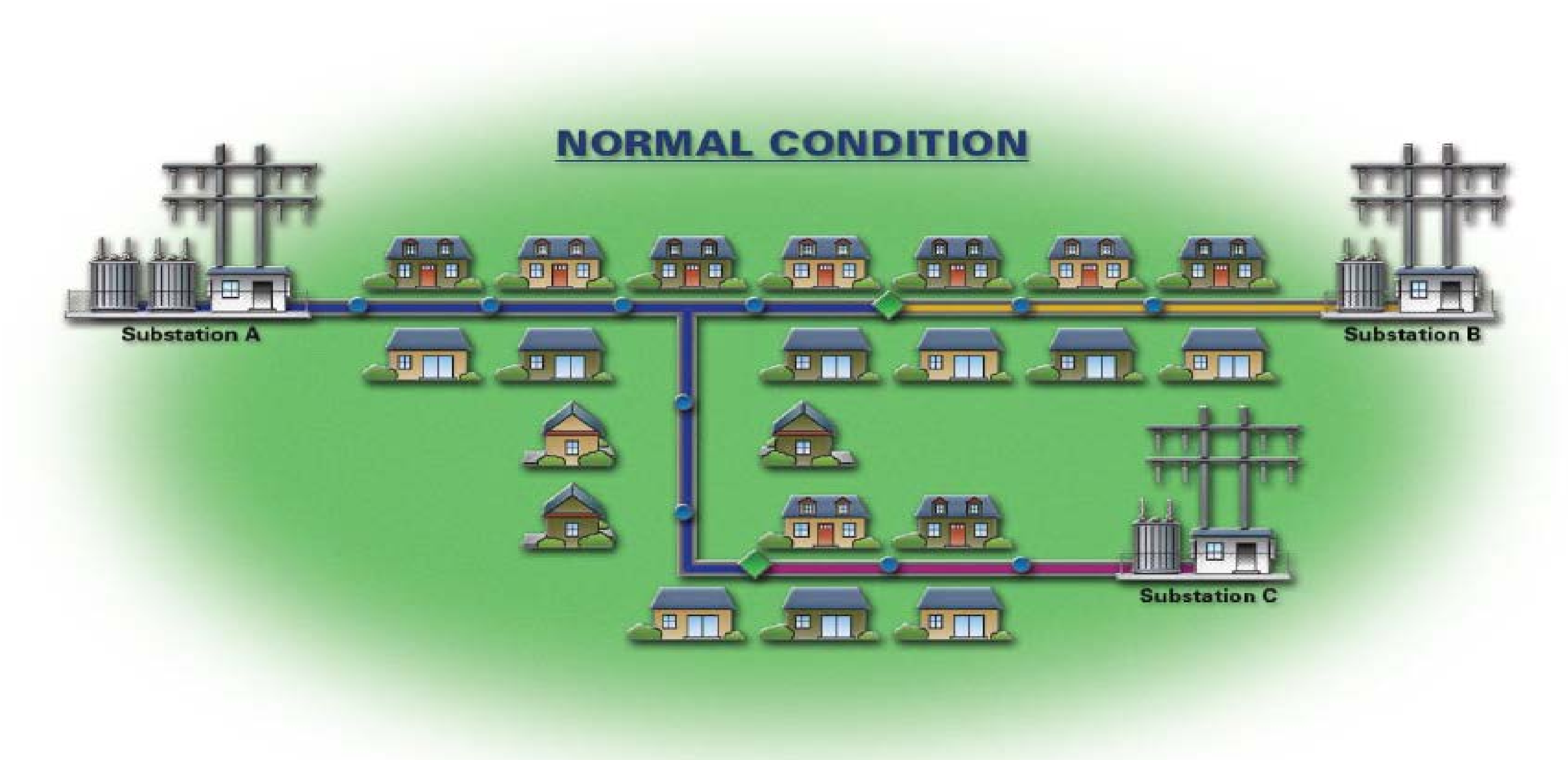
Substation pilot architecture

~150 feet from regulators to control house

- Wireless unit installed in each control cabinet
  - Throughput still more than 1 Mbps
  - Signal adjusted to not be visible or easily detectable outside of substation
- Connection between regulator control and bridges is via Ethernet
- The wireless units at the regulators communicate to a gateway mounted outside the control house
- The gateway connects into a communication switch to an automation control unit
- Engineers can also access individual controls over WiFi

ABB

Outage restoration example
All customers have power



Source: Avista

Outage restoration example
Customers between Substation A and tie points lose power

Source: Avista

Outage restoration example
Power restored from substation A to switch nearest fault

Source: Avista

Outage restoration example
Power restored from substations B and C to switches nearest fault

Source: Avista

Conclusions

- Wireless broadband distribution area communication networks enable smart grid applications
- Optimally, wireless DANs employ a mix of mesh and PTMP
- Successful DAN characteristics
  - Standards-based
  - Resilient, high-availability architecture
  - High throughput and low latency
  - Multi-layer security
  - One network able to support many applications
    - Application-based Quality of Service (QoS)
    - Application traffic segmentation
  - Easy to operate and manage
  - Scalable to economically cover small areas to thousands of square miles
- Wireless DANs proven in scores of utilities throughout the world

This webinar brought to you by the Relion® product family
Advanced protection and control IEDs from ABB

Relion. Thinking beyond the box.

Designed to seamlessly consolidate functions, Relion relays are smarter, more flexible and more adaptable. Easy to integrate and with an extensive function library, the Relion family of protection and control delivers advanced functionality and improved performance.

Thank you for your participation

Shortly, you will receive a link to an archive of this presentation.

To view a schedule of remaining webinars in this series, or for more information on ABB’s protection and control solutions, visit:

www.abb.com/relion

Power and productivity
for a better world™

ABB