White Paper

Building Resilient Wireless IP Broadband Networks with TropOS Mesh Routers

Wireless broadband communication networks play a central role today enabling a wide variety of mission-critical applications across a broad set of industries and environments. Increased adoption of the Internet of Things, Services and People (IoTSP) for remote monitoring and control of business operations, and connectivity for mobile workers, has accelerated demand for wireless communication networks that are highly resilient.

ABB Wireless has over ten years of experience during which it has deployed more than 1,000 wireless broadband mesh networks used by utilities, oil and gas fields, and mining operations. Resilience is a requirement shared among these disparate customers due to the critical nature of their applications. TropOS networks employ a highly resilient self-organizing mesh architecture that resists and recovers from a variety of conditions that could otherwise disrupt normal operation.

A resilient system is defined by two key attributes: continuity and recovery. Continuity is the ability to withstand the impact of an unexpected incident and continue normal operation. Recovery is the ability to automatically return to a normal operating state after an unexpected disruption.

Where network resilience matters

Wireless IP communications are increasingly becoming commonplace for many types of mission-critical IoTSP applications; and resilience is one of the key criteria for these use cases. Examples of such networks and applications include:

Utilities (electric/water/gas) – Utilities have responsibility for delivering a vital service to a territory that can span a few square miles to hundreds and even thousands of square miles. The services they provide are essential for day-to-day operation of businesses and households and customers expect them to always be available.

Many utilities have installed smart grid applications to improve their operational reliability, security, and efficiency. A smart grid requires two-way communications to enable remote monitoring and control of a wide variety of intelligent field devices. The communications capability allows them to deliver more reliable service and also enables them to recover from outages faster–they can quickly identify and isolate problems and dispatch personnel, coordinate

restoration activities after a service outage, and reduce downtime. Utility field workers can also connect to the network for trouble tickets, scheduling, email, and many other applications. Smart grid communications for electric utilities enables a number of new applications including fault detection, isolation and recovery/fault location isolation and service restoration (FDIR/FLISR), Volt/VAR optimization (VVO), conservation voltage reduction (CVR), substation automation, automated metering infrastructure (AMI), distribution automation (DA), outage management, automatic load shedding, access security monitoring and control and video security. Water smart grid applications include AMI, leak detection sensors, tank sensor monitors, access security and video security. For gas, smart grid applications include AMI, gas leak sensors, access security and video security.

Oil and gas fields often span large geographic areas in remote locations and operate 24/7 year round. Many of these fields experience extreme weather conditions at different times of the year – heat, high humidity, wind, dust, rain, salt fog, cold, and snow. Remote control and/or monitoring of oil rigs and well pad devices enables operators to verify normal activity and to receive alerts that if not addressed, could result in critical conditions such as leaks, fires, and explosions. Operations may use video monitoring to increase situational awareness and security. Drill rigs require precision monitoring and control, analysis, and diagnostics and are monitored centrally for optimizing production and safety. Field workers use the network to access operational data and communicate with each other. Oftentimes they are in the field alone in remote locations and the ability to communicate can be critical in emergencies and for personnel safety. For all of these types of applications, the network must offer resilience to unexpected problems.

Mining operations – Mining operations are typically located in remote areas that can span tens to hundreds of square miles. Private wireless networks have become a critical element in modern mines and support a range of applications related to operations and safety. For example, centralized monitoring of key mining equipment telemetry (tire pressure, engine temperature, gas gauge, etc.) is used to help in preventative maintenance planning, reducing downtime and increasing uptime. On-the-fly material analysis provides operations with visibility into substances as they are being mined, identifying early problems and assisting in planning processing. Video cameras are mounted at the site of active mining operations, allowing plant operations real-time visibility into activity, increasing efficiency and safety. Video is also used for perimeter security enabling many remote locations to be centrally monitored. Since active mining sites are continually being reconfigured, a network needs to have the flexibility to be easily deployed and relocated with minimal disruption to service. Oftentimes voice and data communications is used by mobile mine workers to facilitate operations and coordination with other workers.

In order to support these mission-critical roles, the communications network needs to offer resilience, providing both continuity in service and fully recovery if an unexpected incident occurs.

Challenges to building resilient wireless broadband networks

Wireless networks are typically faster to deploy and less costly compared to wired alternatives. However, there are some unique challenges when it comes to designing and building resilient large-scale outdoor wireless networks. Some of the challenges stem from inherent characteristics of the wireless medium

that is lossy, variable and prone to interference. Others stem from the unique challenges of industrial-class outdoor networks including harsh environmental conditions, exposure to extreme weather events, mechanical failures and power outages. Finally, there are growing concerns about risk of cyber security threats to critical infrastructures.

Wireless has its unique challenges, especially having to do with maintaining reliable connections under dynamic and unpredictable outdoor operating conditions. These wireless-specific challenges include: unlicensed and shared frequency bands; limited radio spectrum; RF power and propagation constraints in the outdoor environment; effects such as shadowing, fading, multipath and mobility; and various forms of interference that can adversely affect wireless links.

In addition to the wide range of wireless-specific effects, there are a number of other variables that can impact the reliable operations of wireless broadband networks. Power outages can affect communications equipment and, depending on whether or not there is backup power or storage, disrupt the communications networks. Extreme weather events such as hurricanes and storms can bring down power lines, cause flooding in underground vaults and otherwise render communications equipment inoperable. In addition, cyber security threats are growing in number and breadth, and they have the potential to disrupt communications and cause significant damage to devices and equipment, as well as break of confidential information.

These examples highlight some of the challenges a resilient wireless broadband system needs to address in order to resist these unforeseen events, adapt to the changes, continue to maintain service even under adverse conditions and return to normal operation after a disruption is over.

Customers' resilient TropOS broadband mesh networks

At ABB Wireless, we have more than a decade of experience designing and deploying wireless mesh solutions in large-scale outdoor settings. Our customers include utility customers such as the Abu Dhabi Water and Electric Authority (ADWEA) which operates a 600-square-mile TropOS network for Advanced Monitoring Infrastructure (AMI) electric and water meters, as well as other demanding smart grid applications including distribution automation and substation automation[1].

Avista[2], an investor-owned utility headquartered in Spokane, Washington, has deployed TropOS mesh network to support smart metering as well as feeder automation and Volt/VAR optimization projects[3].

In a remote Eagle Ford oil field, a TropOS network is used to support mission-critical SCADA communications enabling field automation and more efficient operations[4]. Today the network is comprised of more than 1200 TropOS routers. In addition to SCADA, the network provides communications for mobile field workers, helping ensure their safety.

PotashCorp uses a TropOS mesh networks to support multiple applications at two of its open pit phosphate mine locations providing the mine control center with real-time access to data and video from active mining pits[5]. To help in planning preventative maintenance, dragline telemetry is monitored centrally, reducing unplanned downtime. Video cameras are also used for perimeter security and monitored centrally.

Ten key resiliency attributes of TropOS networks

ABB Wireless has designed a highly-resilient mesh network architecture and integrated a number of high-resiliency features into its line of TropOS wireless products. To demonstrate some of these attributes in this section, the descriptions are supplemented with real-world data gathered from a customer's 500-router network located in the Midwestern United States. The network covers a small city of approximately 18 square miles. Figure 1 shows a geographic view of this network (the underlying map has been suppressed to preserve the customer's confidentiality).

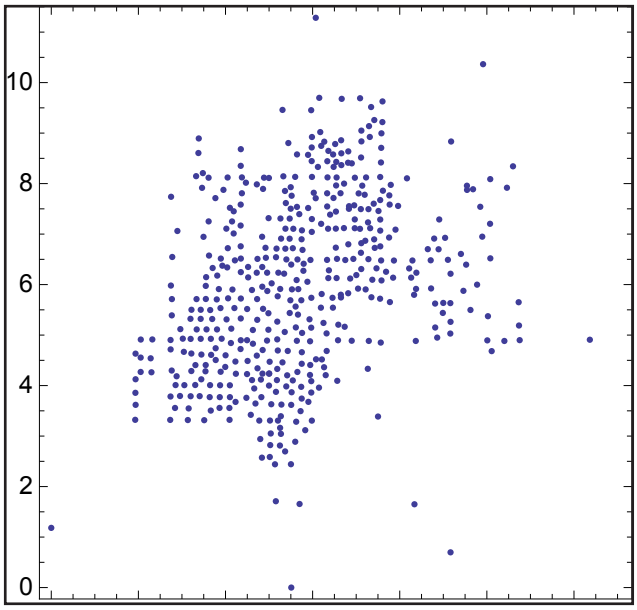

Figure 1 Geographic distribution of 500 TropOS routers covering roughly 18 square miles

1. Dynamic Routing: ABB Wireless utilizes a mesh architecture (Figure 2) such that each node has multiple connections and paths. The company developed its own mesh routing protocol, Predictive Wireless Routing Protocol (PWRP™), which continually analyzes the quality of active and inactive mesh links to select the best path for network performance.

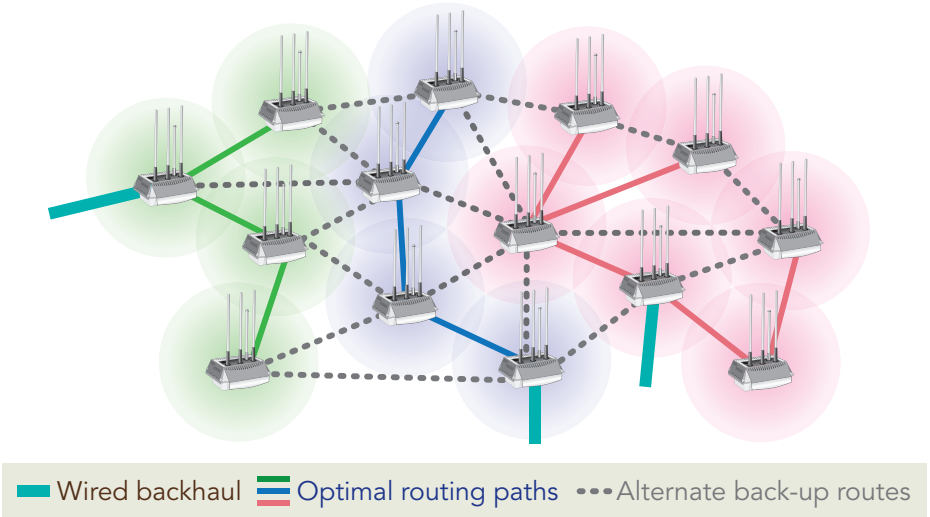

Figure 2 TropOS mesh architecture

Optimal links are selected based on throughput, latency, packet success rates, and other key criteria. With PWRP, TropOS routers dynamically

route around failures and adapt routes in real-time to optimize end-to-end network performance. The underlying routing algorithm is capable of detecting failures, at the level of individual routers or links or at the level of faulted subsystems, and selecting alternate paths that avoid the problem, resilient and seamless connectivity. Even if a backhaul link fails, the adaptive clustering algorithm allows the network to adapt and reconfigure itself around the surviving backhaul points.

PWRP routing is able to deliver resilience benefits by leveraging the diversity of alternate links that exist for each node in a dense mesh network. Figure 3 illustrates the concept of routing link diversity – the median router in this network has 4.3 neighbors while 11% of the nodes have more than 8 neighbors. Since these alternate choices are often spatially separated, their failures will often be uncorrelated. The PWRP routing algorithm intelligently and dynamically selects between the alternative paths, avoiding outages.

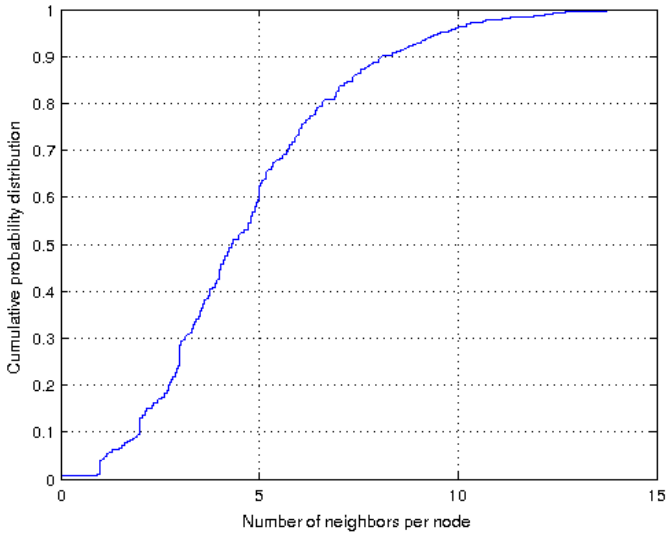

Figure 3 Cumulative distribution function of router neighbor counts

2. Automatic Interference Avoidance: Automatic Interference Avoidance is a distributed algorithm, developed by ABB Wireless to continuously monitor channels available on each link for interference or congestion. By monitoring and assessing alternate channels, Automatic Interference Avoidance allows each node to dynamically and seamlessly switch to a more optimal channel. This ability contributes to maintaining network performance even in a highly-dynamic RF environment.

   Similar to dynamic routing, individual wireless links between transmit and receive antenna combinations are evaluated (through transmit and receive diversity techniques), in the frequency domain (through automatic channel selection within a frequency band as well as selection of operating frequency band), in the time domain (Automatic Repeat Request (ARQ) and retransmission schemes), etc. The automatic channel selection algorithm can optimally distribute the mesh links across available channels so as to maximize system capacity.

   Figure 4 demonstrates with data from a real-world network how TropOS Automatic Interference Avoidance exploits the available channel choices (in this case, channels 1, 3, 6, 9 and 11 in 2.4 GHz) and distributes usage across these choices to maximize system capacity while also maintaining reliability. The flexibility of channel choices within the system translates to greater resiliency and performance optimization.

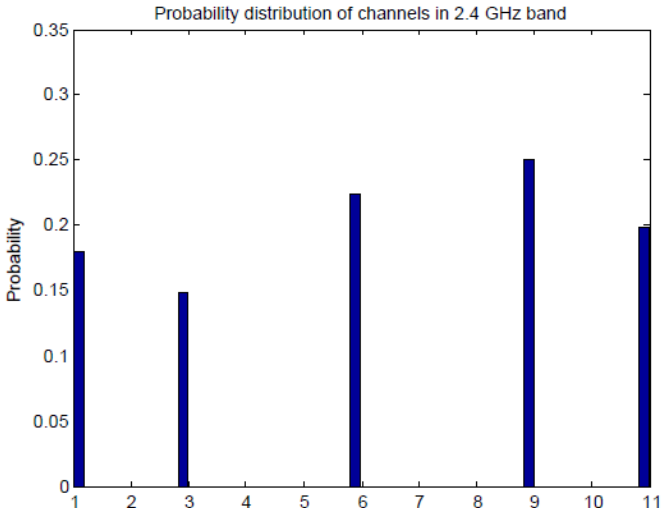

Figure 4 Percentage of 2.4 GHz mesh links on each of the available configured WiFi channels

3. Dynamic transmit power control and adaptive modulation: PowerCurve is a distributed algorithm that maximizes network performance and capacity by automatically optimizing power and transmission rate parameters on a per-connection and per-packet basis. By allowing links to dynamically adjust their output power levels and adapt the modulation rates, it maximizes the operability and availability of the wireless and thereby increases the reliability and resilience of the network.

4. Multi-layered security: ABB Wireless offers a layered defense-in-depth approach to security that utilizes multiple independent security mechanisms. It is generally accepted that a multi-layered scheme for security is the most successful defense against a wider variety of attacks. For example, physical security through tamper detection and mitigation at the device level is complementary to air-link encryption and to end-to-end security measures at the application layer, and these measures, when taken together, make the overall system more resilient. Figure 5 illustrates an overview of how ABB Wireless has implemented security across multiple layers of the protocol stack [5].

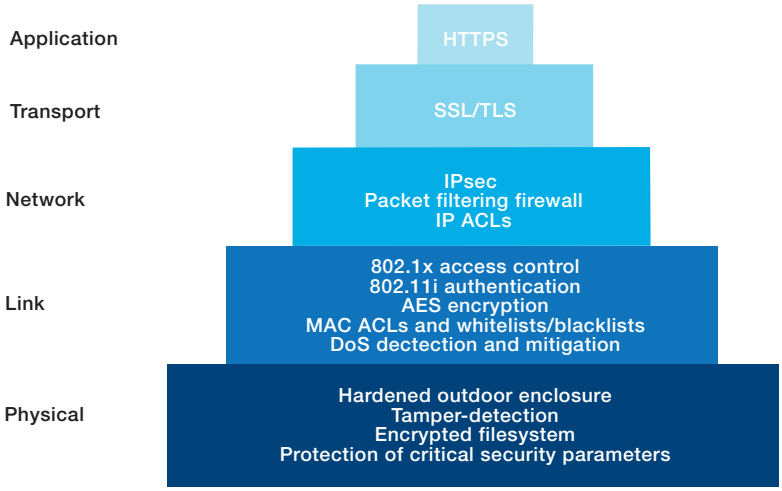

Figure 5 TropOS Multiple layers of security

5. Threat containment: In the event a TropOS node is compromised there are mechanisms in place to quarantine the affected device(s), isolate them from the rest of the network and minimize the impact on the rest of the network.

By doing so, the remainder of the network can continue operating and off-line nodes can be dynamically routed around.

To isolate a threat there are multiple mechanisms employed, including partitioning and segmenting different application flows, firewalling different device types from each other and restricting the set of services accessible to each device or application class. For example, if one class of devices is compromised, the extent of damage to the rest of the system is limited by the restricted access afforded to each category. TropOS routers also have the ability to detect intrusion attempts and initiate mitigation steps including event reporting and lockdown of interfaces suspected of having been breached.

6. Quality of Service (QoS): ABB Wireless enables a TropOS network operator to configure rules that prioritize network traffic. Such prioritization may be important for normal day-to-day operations or to ensure the most critical applications are afforded higher priority over less critical traffic in emergency situations.

   For example, a utility will want to ensure specific applications that have low latency requirements, receive vs priority those that are less latency sensitive such as AMI.

Connected Applications	Latency Requirements
– Data Center Tier 1 apps and DR, PMU, – Substation RAS, EMS – Operations Center – Substation Automation Protection & Control – Protective Relaying – SCADA Masters – Metering Backhaul	Very Low
– Large Distribution Substations – Telephone/radio – Video – Substation Automation Protection & Control – SCADA – DMS	Low

ABB Wireless offers the operator the flexibility to configure QoS based upon multiple parameters including: by applications, 802.1p/802.1q, SSID, by connecting device type (wired or wireless). In addition, dynamic rate limiting features allow the operator to limit network usage by client devices to a certain level and once they reach the limit, reduces their capacity so that no single user dominates bandwidth usage. These features allow the network to continue operating and maintain essential services even during extreme conditions and high-utilization scenarios.

7. Fallback mode: To help achieve system resiliency, TropOS offers IT the ability to configure a set of fallback modes. This enables the system to automatically take action to trade off performance for continuity of service by dropping down to a lower rate or to a reduced-performance feature set. For example, a multi-band TropOS node may be configured to utilize 5 GHz links where possible for performance reasons, but may fallback to 2.4 GHz connections where necessary (see Figure 6 for an example cluster containing one mesh link (in green) that has fallen back to 2.4 GHz). Such a system is more resilient than a system that is exclusively reliant on using 5 GHz to connect mesh routers with each other.

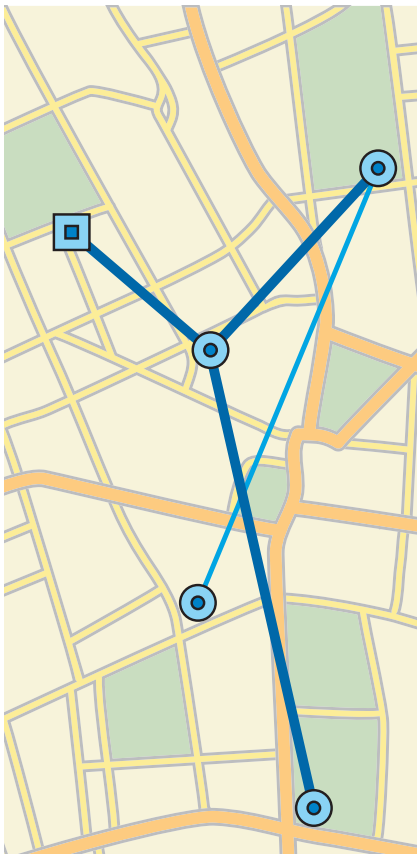

Figure 6 TropOS Mesh cluster with a mix of 5 GHz links (thick blue lines) and 2.4 GHz links (thin light blue lines)

Another example of how TropOS fallback modes is used to increase system resiliency is when the network experiences transient conditions such as fades or multipath variations. By deploying intelligent algorithms for adapting transmission power and modulation rates to help mitigate these effects, ABB Wireless allows affected links to temporarily drop to lower data rates or operate at higher transmit power levels in order to maintain uninterrupted connectivity.

8. Hot failover: For applications that demand close to 100% uptime, TropOS offers several types of hot failover in both hardware and software. For example, two gateway TropOS routers can operate concurrently, both routing traffic. If one gateway fails, the second router immediately associates with nodes that had been connected to the failed router, taking over forwarding of packets with minimal disruption to normal operation. When the failed router comes back on-line, nodes re-associate with it automatically.

Similarly, the SuprOS network management system can be configured with more than one instance on the same network. Should one SuprOS server fail, the second automatically takes over without service disruption. ABB Wireless also offers the option of battery backup for TropOS routers that provide the ability to ride out power outages of up for several hours, enabling the network to maintain operation.

9. Physically hardened hardware: In addition to the ruggedized design of most TropOS routers, some offerings are specially hardened to be resilient against specific harsh conditions. Such units include a ruggedized enclosure designed to withstand a wide range of challenging outdoor environmental conditions such as extreme temperature, weather events such as dust storms and hurricane winds, lightning strikes, impact, submersion, etc.

   Figure 7 provides a list of physical environmental protections that ABB Wireless TropOS routers support:

Environmental Condition	Protection Level/Design Standard	Description
Environmental Protection	IP67	Certifies that units are dustproof and can be submerged in 1 meter of water for 30 minutes without damage.
Shock & Vibration	ETSI 300-19-2-4 spec T4-1E class 4M3	All fixed TropOS routers meet this specification for shock and vibration. In addition, the TropOS 4310-XA mobile router meets EN50155 and its shock and vibration spec EN61372 which are specs for railway rolling stock.
Electrical protection	EN61000-4-4 Level 2 electrical fast transient burst immunity EN61000-4-3 Level 2 EMC field immunity EN61000-4-2 Level 2 (contact), Level 3 (air) ESD immunity	TropOS is in compliance with EMC standards for industrial environments.
Substation Operation	IEEE 1613	TropOS is in compliance with the environmental and test requirements for communication network devices locatedin electric power susbstations.

Figure 7 TropOS physically hardened hardware options

In addition, TropOS router hardware is designed to meet challenging outdoor radio frequency (RF) conditions including in-band and out-of-band interferers and noise sources.

10. Network analytics and performance optimization: TropOS routers are constantly monitoring their local environmental conditions as well as gathering wireless network performance data which is uploaded to the SuprOS network management system. A large class of faults are addressed in normal operation through the automatic and adaptive mechanisms present in TropOS system software (for example, Smart Channel automatically detects interference or elevated noise and enables links to switch to a different channel). However, there will always be a (smaller)

class of conditions that will require operator intervention to remediate. For example, there may be loss of power to a neighborhood resulting in connectivity interruptions. As another example, a point-to-point wireless backhaul link's performance may drop below an acceptable threshold and the solution might be to manually realign the link or replace it with a different kind of backhaul, both of which require physical intervention.

SuprOS provides network health and performance reports that help identify and prioritize these network conditions that require direct operator intervention so that the overall health and performance of the network can be maintained.

Conclusion

ABB Wireless has designed a range of resiliency features into its TropOS wireless mesh network offerings enabling customers to select the right combination for their environment and applications. Router resiliency options may be mixed and matched within a single TropOS network, for example, gateway nodes may be deployed with redundant hardware; nodes deployed in a mine vs at central mining operations may be configured to use different resiliency options. Resiliency options may be needed at different levels in the systems – hardware, software, network and/ component, and deployed individually or together, to make the overall communications network system more resilient.

References

1. ‘The Smart Grid Gets Even Smarter’, Technical Review, Middle East, Vol. 27, Issue 5, 2011, http://www.tpfz.com/pdfs/SmartGrid_Gets_Even_Smarter.pdf

2. ‘Avista: At the Forefront of Smart Grid 2.0’. http://search.abb.com/library/Download.aspx?DocumentID=1KHA-001261-SEN-1000-03.2013&LanguageCode=en&DocumentPartId=&Action=Launch

3. ‘Tropos mesh architecture: A reliable wireless IP broadband distribution area network’, http://search.abb.com/library/Download.aspx?DocumentID=1KHA%20-%20001%20238%20-%20SEN%20-%201000%20-%2008.2012&LanguageCode=en&DocumentPartId=&Action=Launch

4. “Eagle Ford Oilfield Broadband Wireless Mesh Network” http://search.abb.com/library/Download.aspx?DocumentID=1KHA%20-%20001%20303%20-%20REN%20-%201000%20-%2006.2014&LanguageCode=en&DocumentPartId=&Action=Launch

5. ‘PCS Phosphate Company, Inc. (Potash Corp - Aurora and White Springs Agricultural Chemicals, Inc (PotashCorp - White Springs Wireless networks improve mines efficiency and safety”, http://search.abb.com/library/Download.aspx?DocumentID=1KHA-001293-REN-1000-10.2013&LanguageCode=en&DocumentPartId=&Action=Launch

1KHA - 001 367 - SEN - 1001- 11.2016

For more information please contact:

ABB Wireless
3055 Orchard Drive
San Jose, CA 95134
E-Mail: wireless.sales@nam.abb.com

www.abb.com/unwired