CARBON – Ensuring Availability of Wireless Networks

John Anthony B. McVay
Physical Security Pathway

There is a growing need for modern, robust protective networks to guard critical infrastructure or other assets from physical intrusion and attack. These networks must often be deployed where location or time constraints make it impractical to install hardwired data communications by trenching and burying cable. Notable examples include remote or temporary locations and sites with difficult or inaccessible terrain.

A goal of the LWRS Program's Physical Security Pathway is to enable a wireless capability that can provide the framework for continuous, jam-proof, remote-monitoring, and ultimately remote operations of digital systems for both physical security (e.g., sensors, cameras, communications) and safety (e.g., remote-monitoring and operations) at nuclear power facilities. LWRS Program researchers at Sandia National Laboratories have developed a secure and robust communications networking solution, CARBON, which provides highly reliable wireless communications. Just as adding carbon to iron makes hardened, robust steel in networking, joining CARBON network processors to commercial off-the-shelf wireless technologies creates hardened and robust networks. CARBON is ideal for a wide range of applications, including ad hoc wireless networks with limited mobility, fixed-site physical security systems, and rugged-terrain applications.

CARBON supports any communications technology that can send and receive data via a standard Ethernet cable (wired or wireless), enabling the platform to meet a wide range of site-specific needs, as observed in Figure 5. CARBON processors carry large data volumes, such as high-definition live video feeds, as well as different types of sensor and assessment data. Platform-specific alarms, events, and logs provide situational awareness of network health. CARBON can offer the following benefits when it comes to security, versatility, and efficiency.

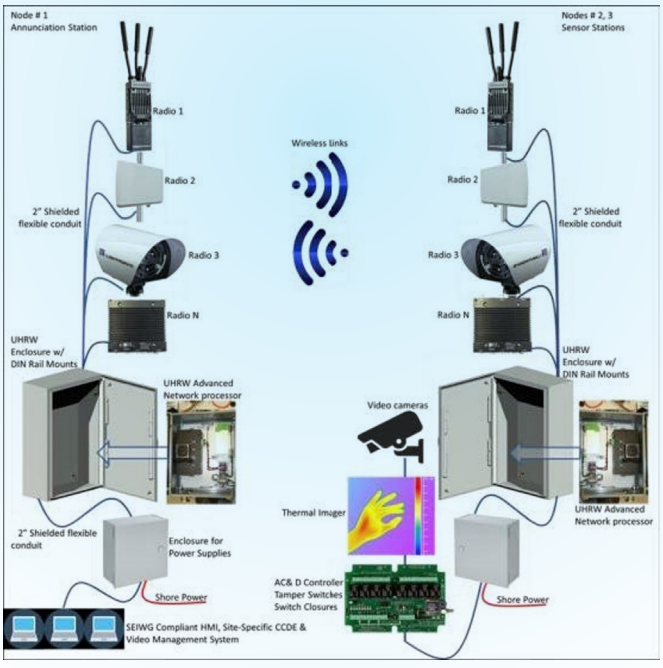
Security

The main goal of CARBON is to approach the security and reliability associated with hardwired communications. CARBON is highly reliable and jam-resistant through its deployment of multiple, redundant, and widely diverse communication layers. CARBON data is protected using the latest Commercial National Security Algorithm Suite encryption, which protects not only against eavesdropping on transmitted data, but also provides mitigations against cyber-threats.

Versatility

Because CARBON supports multiple, redundant wireless technologies, CARBON is adaptable to all terrain types, and

Figure 5. Commonly deployed network components.



supports communications over rocky, mountainous terrain, as well as in, around, and over bodies of water. CARBON-specific information, such as state of network health or firewall violations, are output in a Security Equipment Integration Working Group (SEIWG)-compliant format meaning that CARBON-specific alarms are plug-and-play with any SEIWG compliant command and control alarm station, and thus, no further system integration would be necessary. CARBON supports various radio types and topologies (e.g., radio-frequency, optical, mesh, point-to-point, point-to-multipoint), and can even support wired infrastructure, such as copper or fiber, where such hardwired infrastructure might already exist.

Efficiency

Since CARBON supports wireless infrastructures, it can provide lower initial installation costs, as well as recurring maintenance and upgrading costs to that of buried infrastructure. Adding redundancies or upgrading equipment can be accomplished simply and effectively. CARBON's ability to provide Power-over-Ethernet (PoE) to the utilized equipment reduces complexity when employing PoE-compliant equipment. CARBON provides the capacity to integrate future technologies and capabilities. Additionally, CARBON can offer unique features including:

- Redundant underlay networks mitigate against communication jamming/interference and denial-of-service attacks, as can be seen in Figure 6.
- Monitoring underlay networks for situational awareness.
- Support of multiple mesh radios, point-to-multipoint, optical, and radio-frequency point-to-point wireless links actively transmit and receive video and alarm data, as well as CARBON-specific data and alarms.
- Reporting when a network is jammed, congested, or is otherwise interfered with.
- Reporting unauthorized traffic attempts on the network (i.e., cyber-attack attempts).
- Reliable communications in RF-denied environments (e.g., during counter-unmanned arial system mitigations).
- Reducing potential insider threat vulnerabilities through containerized admin configuration access.
- Configurations via industry-standard Network Configuration Protocol.
- The capability of meeting site-specific needs related to radio-frequency spectrum backgrounds, data rates, topologies, and configurations.

Through further research and development, LWRS Program could apply CARBON to provide a range of highly reliable wireless communications along with other advantageous capabilities, such as continuous health monitoring of security systems. An initial pilot study of the CARBON wireless capability will be conducted at a collaborating nuclear power plant site in 2023, which will help better understand current issues and constraints.

Figure 6. Multiple, redundant underlay networks.