V.04/25

IMPLEMENTING MACSEC (802.1AE) AT THE EDGE: “LAST FOOT” SECURITY FOR ELECTRICITY DISTRIBUTION

Singel 3 | B-2550 Kontich | Belgium | Tel. +32 (0)3 458 30 33 | info@alcom.be | www.alcom.be
Rivium 1e straat 52 | 2909 LE Capelle aan den Ijssel | The Netherlands | Tel. +31 (0)10 288 25 00 | info@alcom.nl | www.alcom.nl

To protect their high-value and high-profile transmissions infrastructures, many electric utilities companies have largely implemented strong security measures for almost all of their communications using protocols such as Secure Sockets Layer and IPsec. However, at the edge of that grid — where local distribution happens — unaddressed vulnerabilities remain.

Distribution Automation equipment is usually located in remote areas with public access, and many of the cabinets housing control equipment are "head" height providing easy access. Utilities physically secure this equipment with locking doors and other strategies such as intrusion sensors. However, communications between the in-cabinet equipment such as recloser controllers and the communications router are often unprotected, creating an attack vector that is often overlooked. This vector can be exploited by a bad actor to damage equipment and affect tens of thousands of customers in an electrical grid.

To address the potential for network intrusions and damage, and harden the security posture for utilities firms, Digi has worked with SEL and integrated the Media Access Control Security (MACsec) protocol within its products. This solution brief explains how electric utilities can capitalize on this new security feature to better protect their infrastructure.

What Is a Recloser?

In most instances, unplanned electrical outages result from lightning, fallen branches, high winds, or vehicle crashes. The recloser, an automatic, high-voltage switch, senses when trouble occurs and — much like a household circuit breaker — automatically shuts off the power before the outage spreads or before the distribution system suffers damage.

Unlike a household circuit breaker that remains off until it is manually reset, a recloser automatically tests the electrical line to determine whether the trouble has been removed. And, if the electrical fault was only temporary, the recloser automatically resets itself and restores the electric power.

Unacceptable Security Exposure

A typical electrical utility that manages a grid covering hundreds or thousands of square miles might deploy tens of thousands of recloser devices to protect and manage electricity delivery. With Digi routers providing a critical communications link, those reclosers represent a tempting target for hackers and other bad actors who can simply walk up to a utility box at a wayside location hundreds of miles away and tap into the grid's communications.

Physical locks and hardening are important measures, but they're not enough. That's because at the very edge of the network, the "last foot" of communication typically uses a standard Ethernet cable between the router and the recloser control. This data is being passed as plain text. This makes this architecture susceptible to "Man in the Middle" attacks.

The hacker could simply disconnect that cable and subsequently connect to and communicate with the recloser control itself, stealing passwords, reading data, manipulating data, injecting data and issuing false recloser trip commands.

How can utility companies secure that link? Increasingly, the answer is Media Access Control Security — MACsec.

What Is MACsec?

MACsec, also known as Media Access Control Security, is an encryption standard operating at Layer 2 within the OSI model that provides a secure bi-directional communication link. It is defined by the IEEE standard 802.1AE.

Some of the benefits of MACsec include:

- **Interoperability:** MACSec is an open IEEE standard, making it interoperable.
- **Confidentiality, integrity, and authenticity:** The use of MACsec ensures the confidentiality, authenticity, and integrity of Ethernet traffic, protecting data from being tampered with or eavesdropped on without permission.
- **Data encryption:** MACsec can encrypt the data in the Ethernet frame (data in transit) using AES encryption to ensure confidentiality and authenticity, because it cannot be viewed or altered by anyone monitoring traffic on the link.
- **Secure commissioning:** MACsec works with MACsec Key Agreement Protocol (MKA) providing simple secure commissioning process.

- **Data integrity:** MACsec appends an 8-byte header and a 16-byte tail to all Ethernet frames traversing the MACsec-secured link. The header and tail are checked by the receiving interface to ensure that the data was not compromised while traversing the link.

MACsec is used in combination with other security protocols, such as IP Security (IPsec) and Secure Sockets Layer (SSL), to provide end-to-end network security. It is used to protect network-to-network or device-to-network connections.

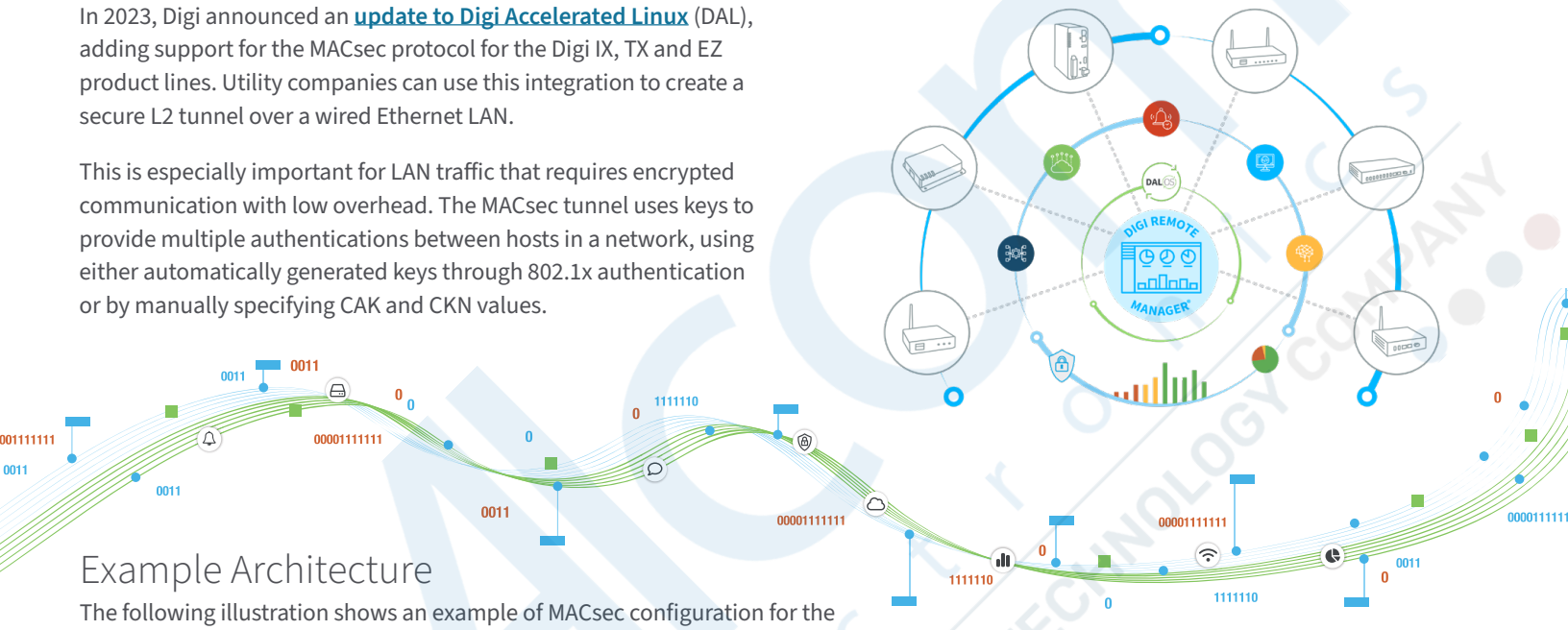
MACsec and Digi Accelerated Linux

In 2023, Digi announced an **update to Digi Accelerated Linux** (DAL), adding support for the MACsec protocol for the Digi IX, TX and EZ product lines. Utility companies can use this integration to create a secure L2 tunnel over a wired Ethernet LAN.

This is especially important for LAN traffic that requires encrypted communication with low overhead. The MACsec tunnel uses keys to provide multiple authentications between hosts in a network, using either automatically generated keys through 802.1x authentication or by manually specifying CAK and CKN values.

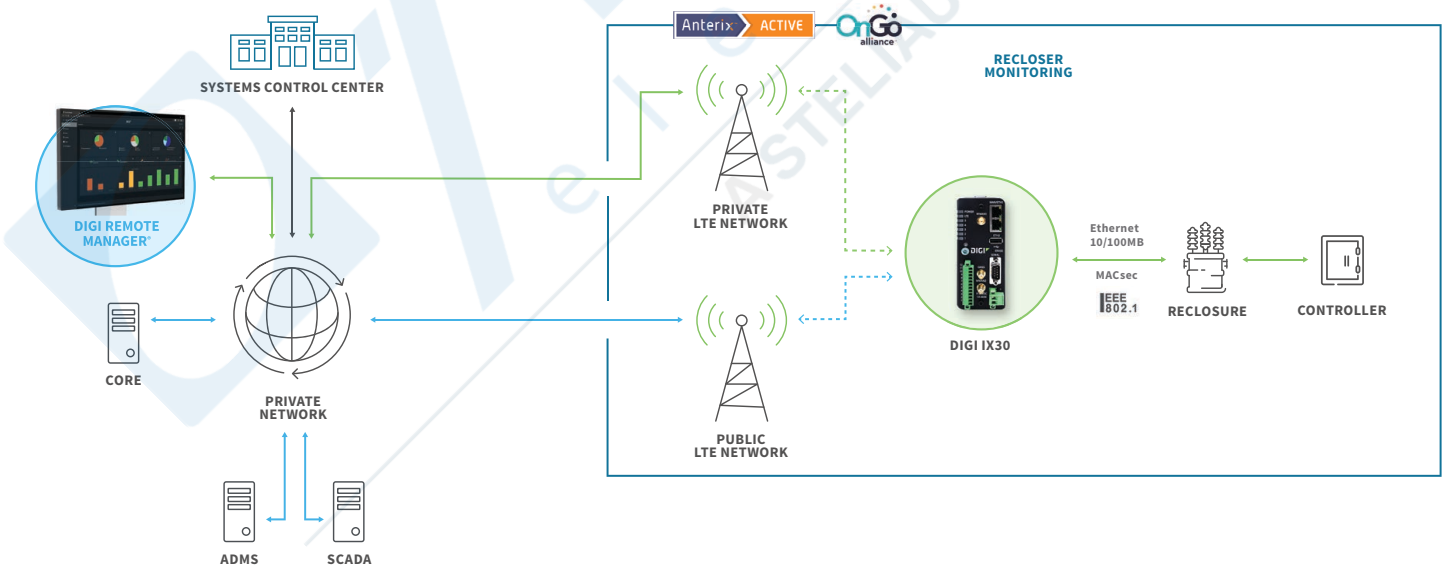
Digi Remote Manager® (Digi RM), the central platform that enables and automates the deployment, monitoring, and management of thousands of devices from a single point of command, plays a central role in managing DAL's use of MACsec.

With Digi RM, you can centrally configure and administer tens of thousands of recloser and Digi router locations and update keys. Digi Remote Manager also offers other tools for monitoring the edge like "Profile Manager." Profile Manager proactively monitors Digi edge routers for any unauthorized changes made to local configurations, reports them to Digi RM and restores the router to the correct state.



Example Architecture

The following illustration shows an example of MACsec configuration for the utilities industry utilizing a hybrid public/private network infrastructure.



Learn More in Our Documentation

To get started configuring MACsec with Digi routers, visit our **technical documentation**.

Why Digi?

Digi is a complete IoT solutions provider, supporting every aspect of your project, from mission-critical communications equipment to design and deployment services to get your application designed, installed, tested, and functioning securely, reliably and at peak performance.

Digi builds its products for high reliability, high performance, security, scalability, and versatility so customers can expect extended service life, quickly adapt to evolving system requirements, and adopt future technologies as they emerge. Digi embedded modules, routers, gateways, and infrastructure management solutions support the latest connected applications across verticals, from the enterprise to transportation, energy, industrial and smart cities use cases.

Our solutions enable connectivity to standards-based and proprietary equipment, devices, and sensors, and ensure reliable communications over virtually every form of wireless or wired systems. Our integrated remote management platform helps accelerate deployment and provide optimal security using highly efficient network operations for mission-critical functions such as mass configuration and firmware updates, as well as system-wide monitoring with dashboards, alarms, and performance metrics.

Company Background

- Digi has been connecting the “Internet of Things” — devices, vehicles, equipment and assets – since 1985
- Digi is publicly traded on the NASDAQ stock exchange: DGII
- Headquartered in the Twin Cities of Minnesota, Digi employs over 800 people globally, and has connected over 100 million devices worldwide

As an IoT solutions provider, Digi puts proven technology to work for our customers so they can light up networks and launch new products. Machine connectivity that’s relentlessly reliable, secure, scalable and managed — and always comes through when you need it most. That’s Digi.

Learn more on our **About Digi** page.