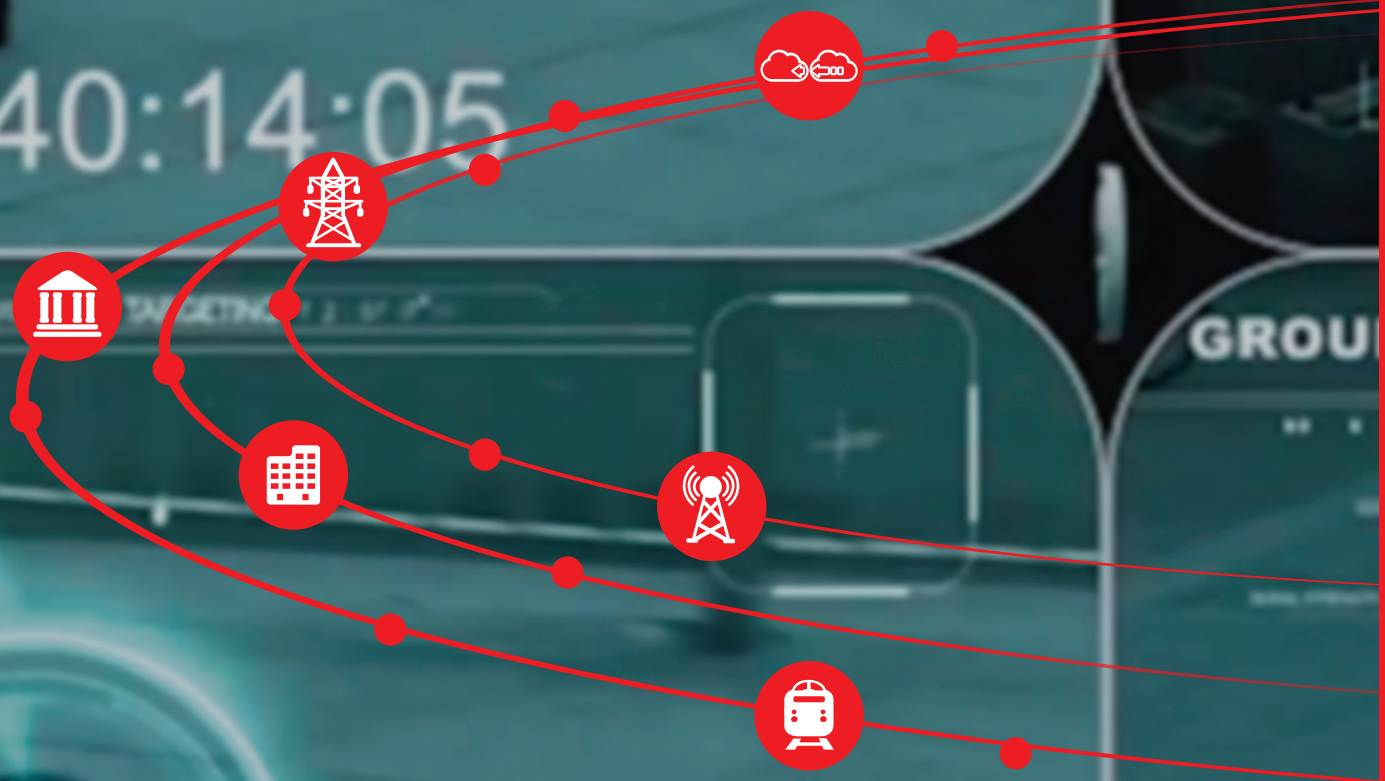
DYMEC
AMERICAN INDUSTRIAL

High Security ITS & Industrial IoT Networking



The Age of Digital Transformation

The industrial internet of things (IIoT) is set to enable digital transformation across all industrial and critical infrastructure sectors. By 2020, IIoT is expected to be a $225 billion market, encompassing millions of highly distributed intelligent devices:

Question - Will your IIOT devices and their network be secure?

Power Utilities

- Smart Grid
- Re-closers
- Load breakers
- RTUs/SCADA
- Secondary substations
- Meters concentrators

Gas Utilities

- Flow meters
- Volume/pressure/level sensors

Water Utilities

- Flow control
- Quality
- Leakage detection
- Pump/valve control
- Meters

Transportation

- Traffic control
- Info boards
- Kiosks

Connected Industry

("Smart Factory/Industrie 4.0/Society 4.0")

- Production floor monitoring
- Remote PLC control
- Automated quality control

Smart Cities

- Smart parking
- Traffic monitoring & control
- Bike sharing
- Smart lighting
- Public safety
- Payment kiosks (PoS)

This signifies a revolution in the industrial world, which is now shifting its focus to increased efficiency and lower costs using smart edge devices and Big Data analytics.



The challenges

Cyber Security Threats

"Intelligent" doesn't equal "protected". IIoT devices' connectivity over unreliable public networks (e.g., the internet) creates countless vulnerability points for hackers to exploit, with potentially disastrous results.

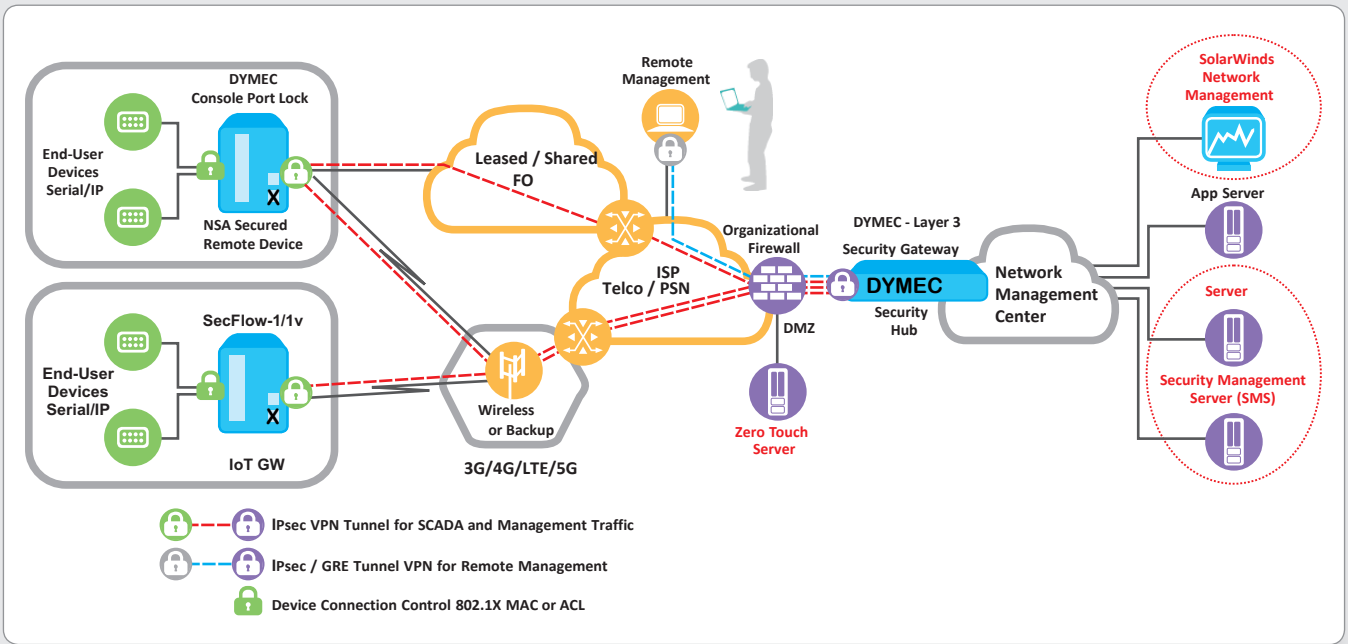
Operational Complexity

High operational costs for provisioning and maintenance/field replacement of thousands of edge devices.

Data Usability

Massive data transmissions to and from IIoT devices in remote sites over diverse network connections in a timely manner is challenging.
That, together with the need for actionable information (i.e., real-time analytics), has led to the growing use of edge/fog computing. Finding the right edge/cloud balance is key to optimize asset performance and costs.

» DYMEC's Secure Industrial IoT Backhaul Solution

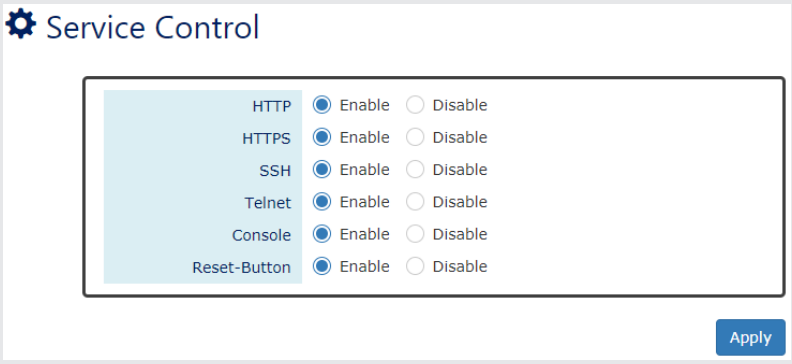


» DYMEC's Service Control Solution

DYMEC offers a comprehensive solution for secure networking for Smart Cities, Connected Industry, Smart Transportation, Smart Energy (generation, transmission and distribution - allowing fast, secure and economical deployment of thousands of new remote IIoT sites with always-on reliability and mission-critical protection.

» Key Benefits

» Easy Configuration
» Control over All Services
» Secure Console Port
» Secure Reset
» Secure Chassis



HTTP

Enable or Disable to access the management interface by **HTTP** - which is the foundation for data communications for the **World Wide Web (WWW)**

HTTPS

Enable or Disable to access the the management interface by **HTTPS**, which is an adaptation of HTTP for security. The communication will be **Encrypted in HTTPS**

SSH

Enable or Disable to access the management interface by **SSH**: a **cryptographic network** protocol. SSH provides a **secure channel** over an unsecured network in the client-server architecture. The switch plays the role of SSH server and hosts plays the role of SSH client.

TELNET

Enable or Disable to access the management interface by **TELNET**: which is a text oriented, virtual terminal connection. Less secure than SSH: it does not encrypt data or passwords.

RESET BUTTON

Enable or Disable to react when users press the **Reset Button.** The Reset Button provides different functions, including **REBOOT** and RESET FACTORY Default. Disabling the Reset Button - provides protection from **System Reboot** or **Restoring the system to a Default State**

NSA Secure Endpoint Console Port & Chassis

NSA Network Endpoint Guideline Certified for Console Port Shutdown & Chassis Full Security (Patent Pending) - Used for High Network Security / IIOT Deployments. This is a Security Feature for Turning OFF or Disabling the Console Port of the Device.

* Fully Secures the Console Port of Remote, Unsecured or Un-Attended Device.
* Prevents Un-Authorized Configuration or Device Penetration via the Console Port
* Secures the Device Chassis and Renders it Secure from Tampering or Virus Placement

NSA Secure Endpoint Console Port & Chassis



Ruggedized ITS & SCADA-Gateway Managed Switches & Routers



Security Switch & Router

Layer3 , Router and Firewall



PoE, Layer 3 Routers & Switches

High Security IIOT Networking

» For more information visit: DYMEC.com

DYMEC and 3170 are registered trademarks of K-USA. ©2019 DYMEC. All rights reserved.