The S4 Group, Inc.

Enhancing and Extending Building Automation Systems

Legacy Building Upgrades and Cybersecurity

FFC OT Security Workshop

The National Academies

Member company

Legacy Buildings Need Love Too

Inventory: 8.6 Million Commercial Buildings

Average Age: 53 Years

▸ Represent 40% of the built environment
- early generation Building Automation System (BAS) and Direct Digital Control (DDC) systems
- many have not been maintained for years
- no Cybersecurity plan.

▸ Most utilize a RS-485 serial interface

The S4 Group {Software Services & System Solutions}

Everyone cares...

But – for different reasons

- Owners care about capital and operational expenses, and occupancy levels
- Occupants care about Indoor Air Quality (IAQ), Safety, Health, Sanitation, Comfort, Productivity
- Manufacturers want recurring income
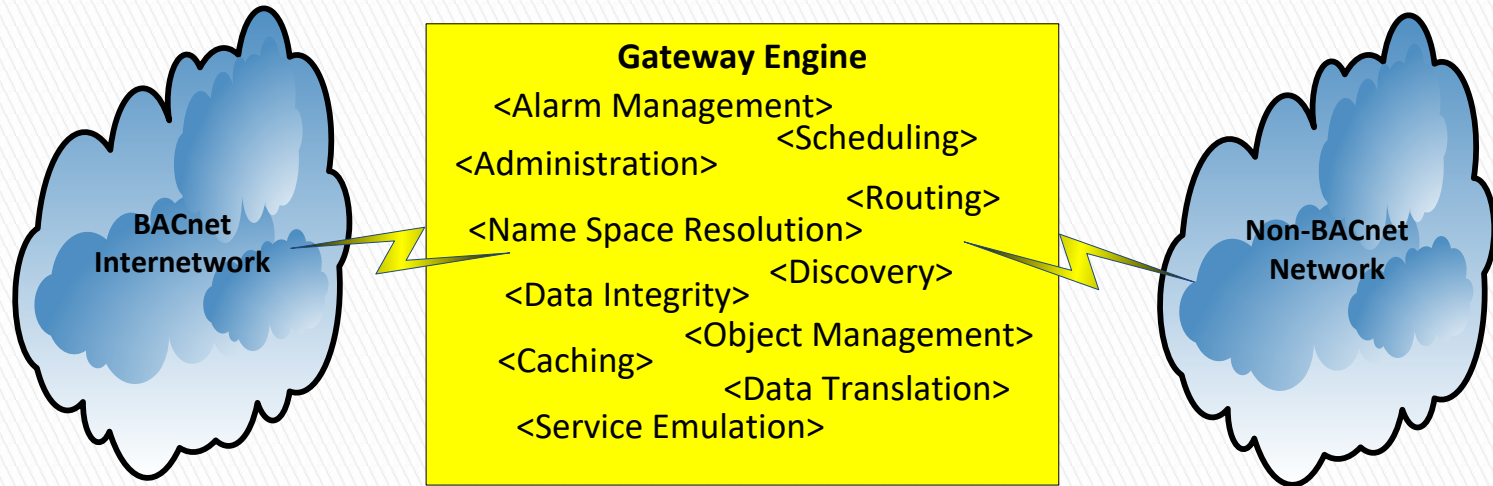- Operators want simplicity

Legacy BAS Installations – The Problem

- Were protected by physical and network isolation.
- Unsecure remote connections and smart phone access opened major security holes.
- May be 25 to 30 years old.
- It's all about risk management.
- No building is too large or too small.
- *Will* eventually need to be replaced.
- **Cybersecurity needs to be a major focus**

The S4 Group { Software Services & System Solutions }

The Logical Solution - Integration

- Owners of large property portfolios cannot afford to upgrade all properties at once.
  - you don't have to rip and replace the BAS in one fell swoop.
  - it can be an incremental process that is executed over time.
- Gateway integration delivers value early
- Paves the way to renewing building infrastructure.
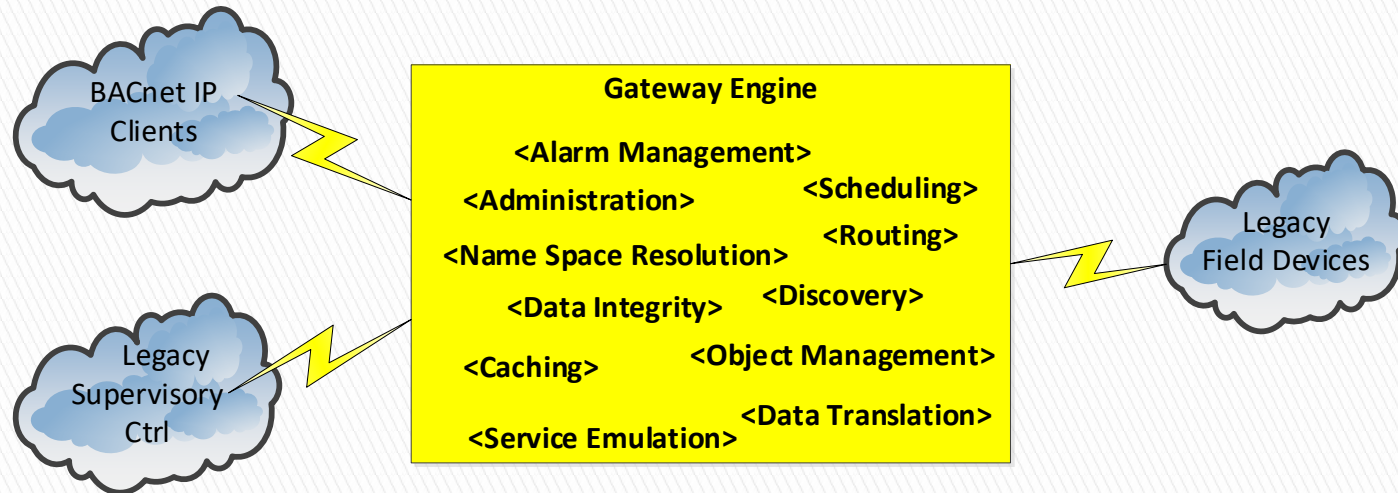- **At each step Cybersecurity vulnerabilities are removed.**

The S4 Group {Software Services & System Solutions}

What is a Gateway?

Gateway Engine

<Alarm Management>
<Scheduling>
<Administration>
<Routing>
<Name Space Resolution>
<Discovery>
<Data Integrity>
<Object Management>
<Caching>
<Data Translation>
<Service Emulation>

BACnet Internetwork

Non-BACnet Network

- BACnet services and interfaces are defined by the BACnet standard
- Nothing is changed in the legacy system
- The gateway provides translation, emulation, security, and isolation
- BACnet is used to normalize and standardize devices and data
- **Only valid BACnet transactions are allowed to access the Non-BACnet network**

The S4 Group {Software Services & System Solutions}

© 2021 The S4 Group, Inc.

Goal: Transparent and Secure Integration / Co-Existence

BACnet IP Clients

Gateway Engine

<Alarm Management>

<Administration> **<Scheduling>**

<Name Space Resolution> **<Routing>**

<Data Integrity> **<Discovery>**

<Caching> **<Object Management>**

<Data Translation>

<Service Emulation>

Legacy Supervisory Ctrl

Legacy Field Devices

- Transparent co-existence with legacy Supervisory systems
- Use case: Replace supervisory level (head end) systems
- Use case: Introduce open BACnet value added applications

The S4 Group {Software Services & System Solutions}

Migration Strategy Review

Salvage

Legacy Field Devices

Manage new & existing equipment from one BACnet interface

Address

Legacy Supervisory Controller

Co-exist with new head end, or Migrate schedules, trends, global variables, and custom logic to BACnet global controller

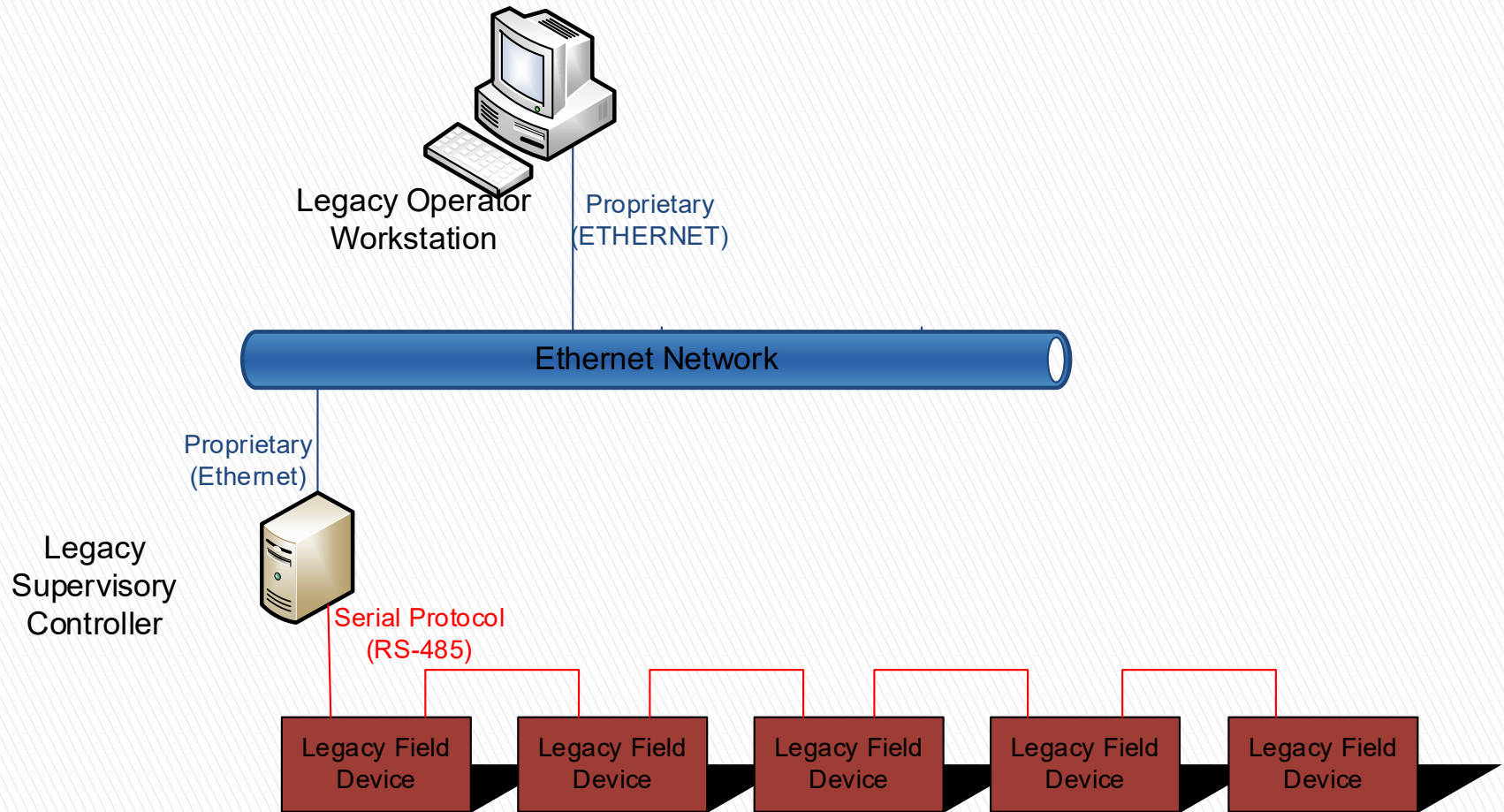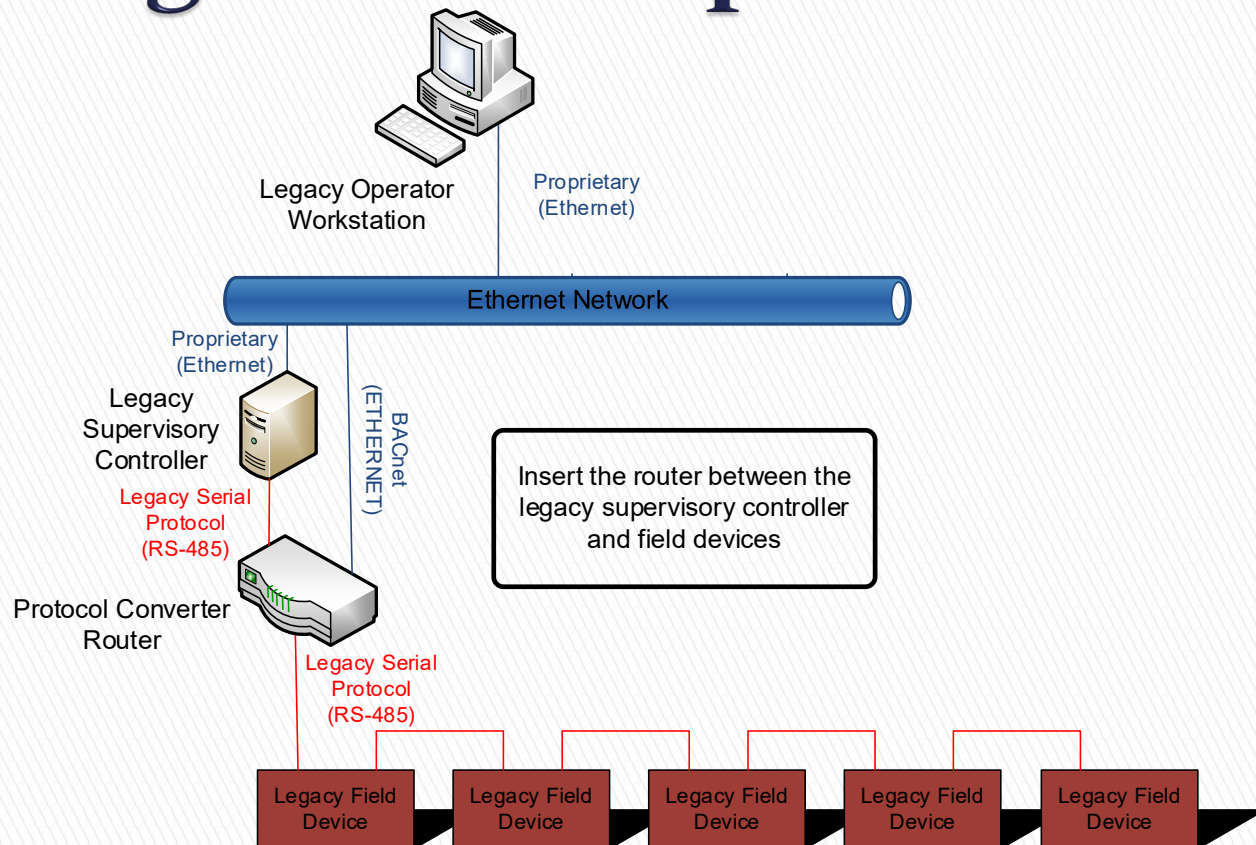**Phase Out**

Legacy Field Devices

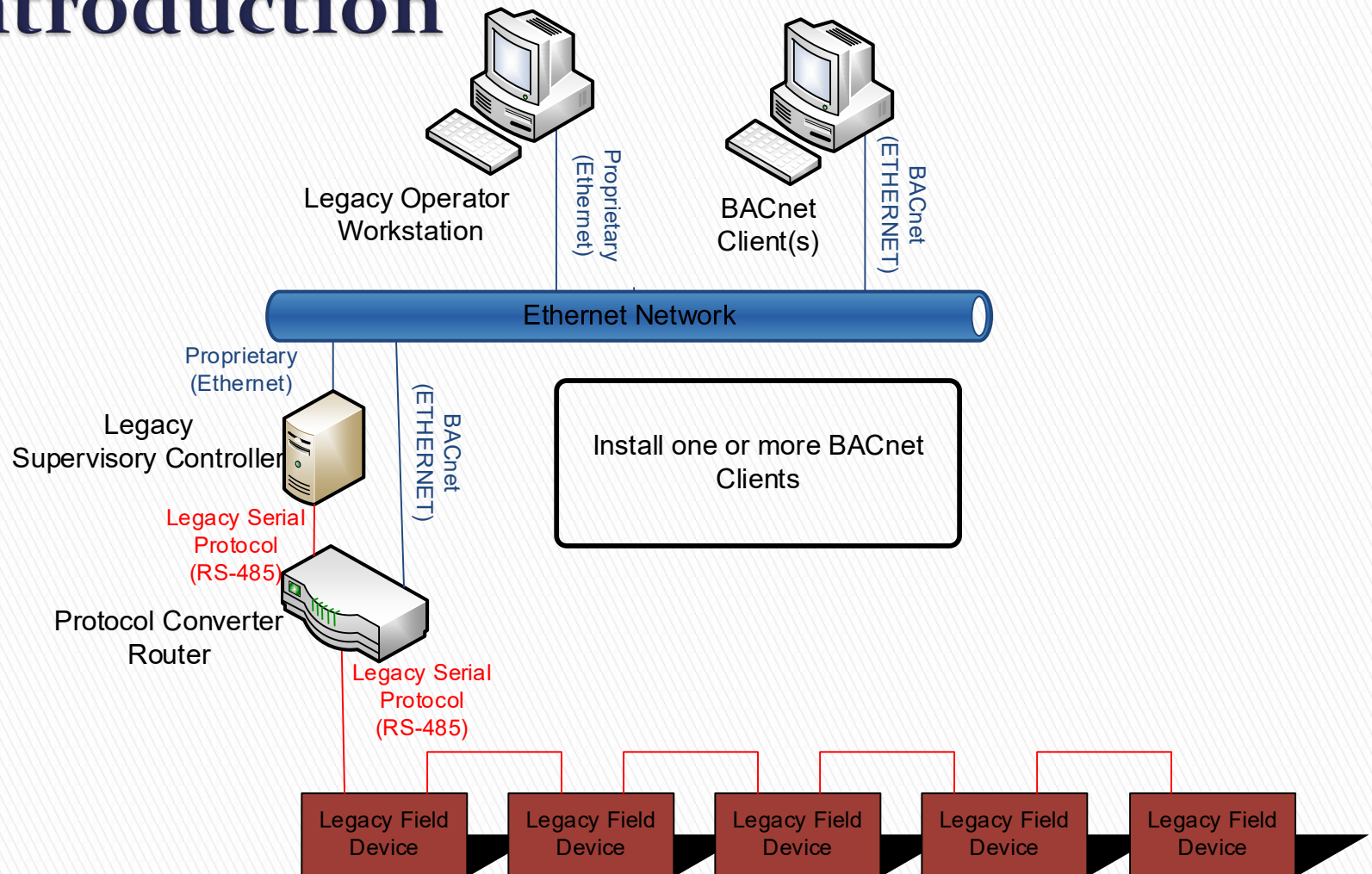Plan strategic replacement of legacy equipment with BACnet controllers over a period of years

The S4 Group {Software Services & System Solutions}

Typical Legacy BAS Installation

Legacy Operator Workstation

Proprietary (ETHERNET)

Ethernet Network

Proprietary (Ethernet)

Legacy Supervisory Controller

Serial Protocol (RS-485)

| Legacy Field Device | Legacy Field Device | Legacy Field Device | Legacy Field Device | Legacy Field Device |

The S4 Group {Software Services & System Solutions}

Integration Step 1: Site Prep

Legacy Operator Workstation

Proprietary (Ethernet)

Ethernet Network

Proprietary (Ethernet)

Legacy Supervisory Controller

BACnet (ETHERNET)

Legacy Serial Protocol (RS-485)

Insert the router between the legacy supervisory controller and field devices

Protocol Converter Router

Legacy Serial Protocol (RS-485)

| Legacy Field Device | Legacy Field Device | Legacy Field Device | Legacy Field Device | Legacy Field Device |

"Investigate Before You Integrate".
- confirm that the legacy field bus is in spec
- confirm all devices are working properly before performing the integration
- this may involve device repairs, replacements, or recommissioning

The S4 Group {Software Services & System Solutions}

Integration Step 2: BACnet Client Introduction

Legacy Operator Workstation

Proprietary (Ethernet)

BACnet Client(s)

BACnet (ETHERNET)

Ethernet Network

Proprietary (Ethernet)

Legacy Supervisory Controller

BACnet (ETHERNET)

Install one or more BACnet Clients

Legacy Serial Protocol (RS-485)

Protocol Converter Router

Legacy Serial Protocol (RS-485)

Legacy Field Device

Legacy Field Device

Legacy Field Device

Legacy Field Device

Legacy Field Device

The S4 Group {Software Services & System Solutions}

11

© 2021 The S4 Group, Inc.

Integration Step 3: BACnet Client Integration

- Treat the legacy systems like open BACnet devices
  - Develop Graphics and navigation for new Operator Workstation
  - Introduce new BACnet global control technology
  - Integrate and configure value added applications
- **Make sure all new technology introduced follows Cybersecurity best practices**
- **Make sure there is a maintenance and support plan for all new technology**

The S4 Group {Software Services & System Solutions}

Integration Step 4: Phase Out Head End
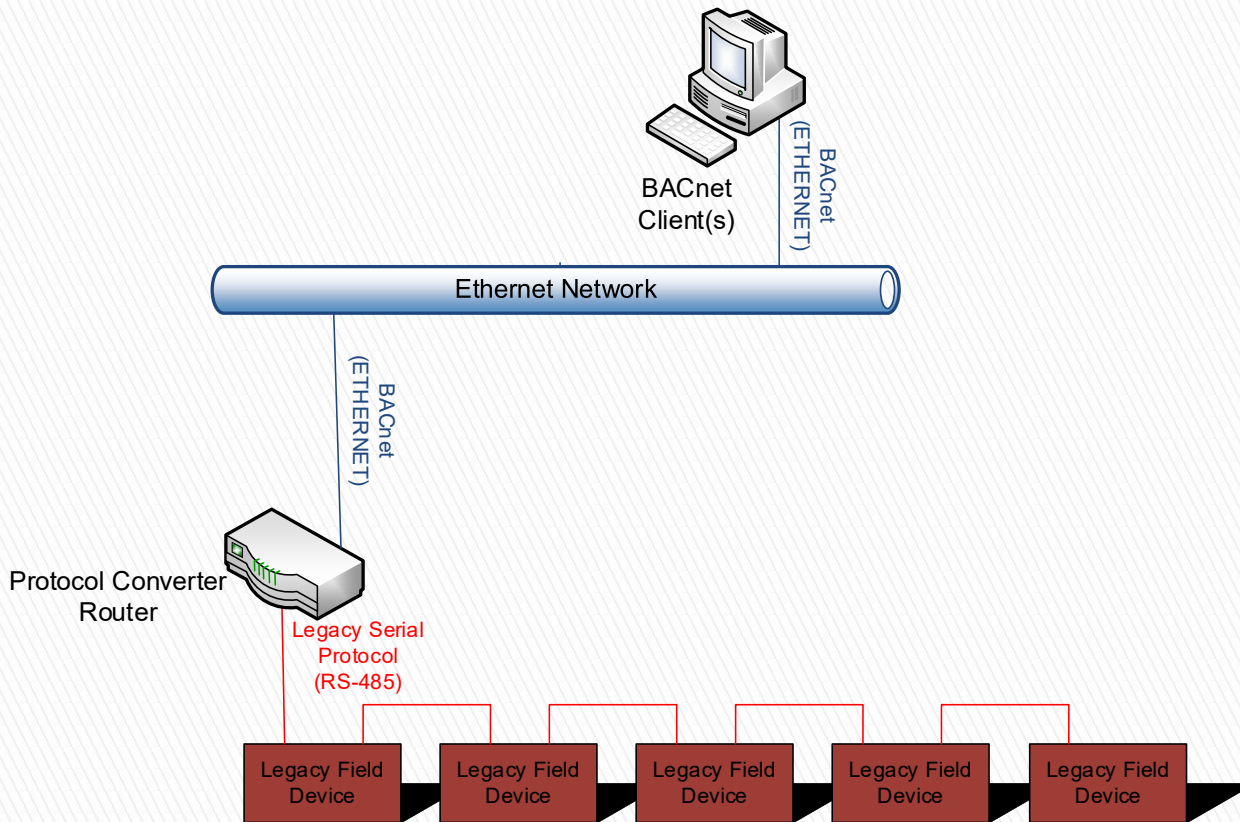
- ► Remove the legacy supervisory controller and operator workstation.
  - o **These are some of the most vulnerable targets for Cyberattacks**
  - o You will need to redefine Schedules, Trends, Global Variables, Custom Logic

The S4 Group {Software Services & System Solutions}

Why BACnet

- **BACnet is an open ASHRAE and International standard utilized by most BAS manufacturers (60% market share)**
  - BACnet embraces the Building IoT concept
  - BACnet promotes competition and interoperability
  - BACnet promotes vendor innovation
  - BACnet International has a stringent and mature certification process for BACnet products
  - **BACnet is continually evolving to meet building automation needs**
- **Introducing BACnet technology starts the migration towards Smart and Secure Buildings**

BACnet – Not Just HVAC Control

- Lighting systems
- Access systems
- Security and CCTV
- Life safety
- Renewable energy sources
- Windows and shading

- Parking facilities
- Irrigation
- Smoke control doors & dampers
- Mass notification
- Elevators
- Emergency power

Buildings Have Personality

- The mission of the organization utilizing a building determines its personality
  - Residential, Retail, Warehouse, Medical / Pharma, Manufacturing, Entertainment, Hotel, Airport, Education
- This determines the type of infrastructure and technology needed in the building to support the mission
- Vertical market networking technology will be introduced to support the infrastructure and technology.
  - OPC, Modbus, and many others. Each with their own Cybersecurity attack surface.

BACnet Secure Connect (SC)

- **A new transport for BACnet services that embraces accepted IT security practices.**
- **Reference implementation available from BACnet International.**
- **It is being adopted by most manufacturers.**
- **Utilizes TCP, TLS, and Certificates.**
- **Managed BACnet is an industry initiative to introduce management capabilities on top of BACnet SC.**

The S4 Group {Software Services & System Solutions}

Cyberattack Prevention

- Start the migration process today
- Conduct a Cybersecurity audit just as you might for IT systems and networks
- Maintain physical access security
- Bridge the chasm between IT and OT organizations.
  - You should both have the same goal. Success of the organization's mission.
- Eliminate all non-secure remote access methods
- Replace unsecure remote access technology with secure remote access technology such as TOSIBOX.

Questions?
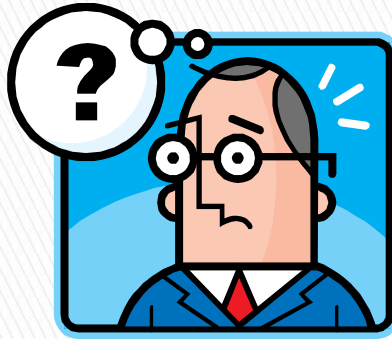
Contact:
Steve Jones
Managing Partner
The S4 Group, Inc.
(801) 621 1970
sejones@thes4group.com
https://www.thes4group.com
https://www.linkedin.com/in/stevejoness4group/

The S4 Group {Software Services & System Solutions}