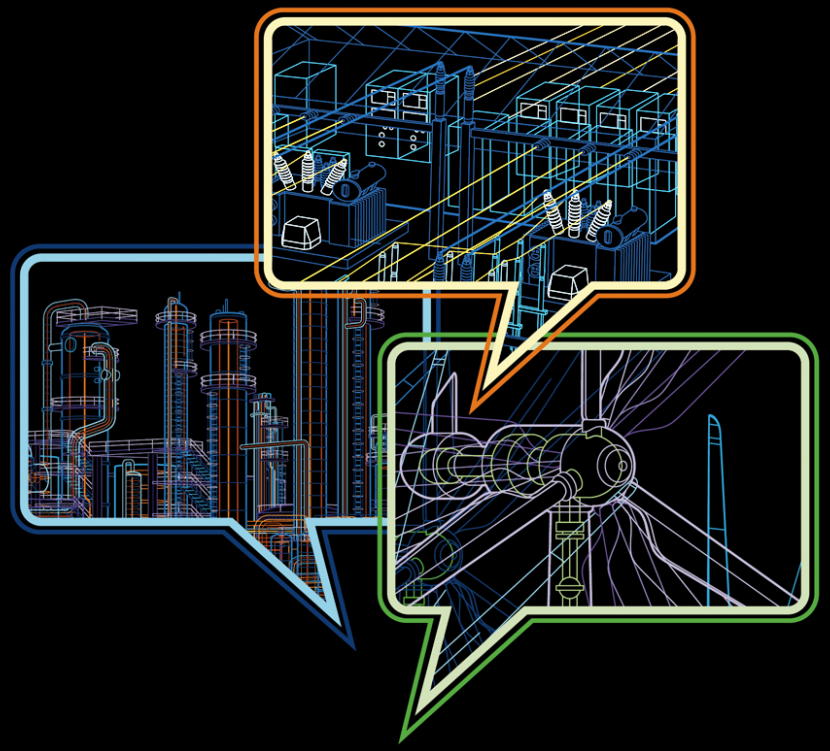


Engineering Your Substation Network for Protective Relaying, Automation and SCADA

Jim Bougie, Regional Technical Manager – Midwest - ABB

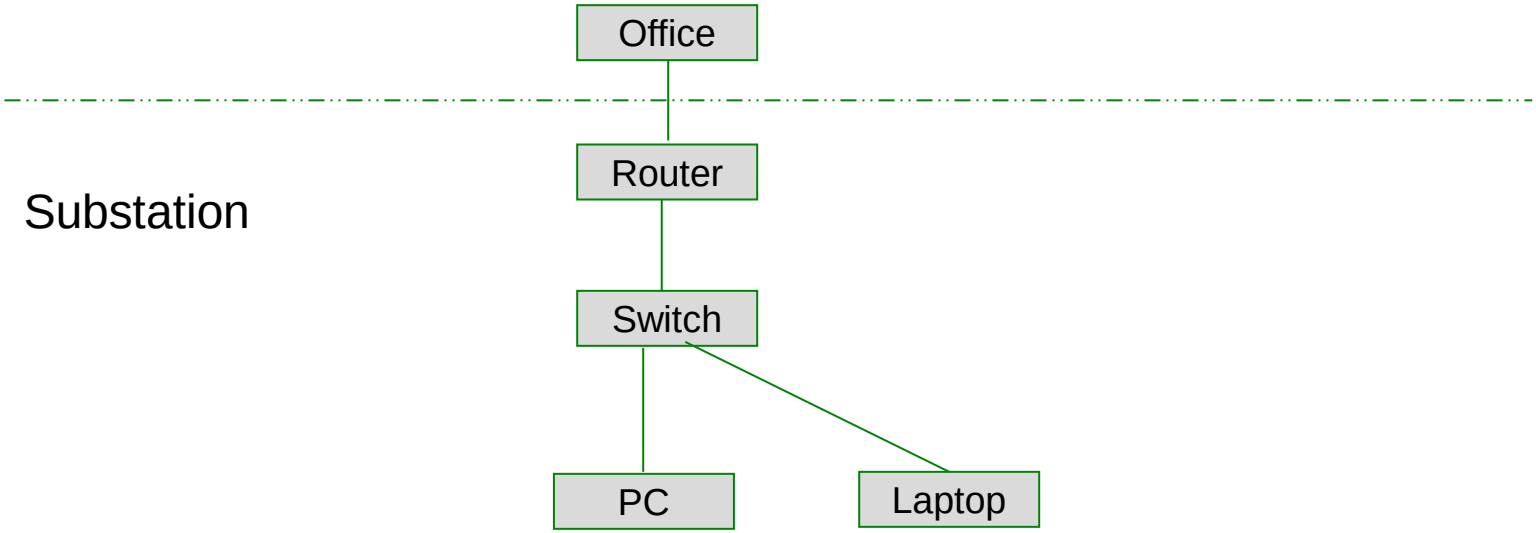
Agenda

- Types of Networks
- Network Design
- Network Concerns

Network types - Enterprise

- Used to access business applications
  - Email, Time reporting, etc
- Typically can be the same as a typical office network
  - No need for redundant networks
    - If the network fails, you can wait for it to be repaired
  - Do need to use substation harden equipment
    - All equipment needs to be designed for the environment used.
  - These systems are design to handle interruptions
  - Routers are needed for security reasons
    - These devices are designed for providing security

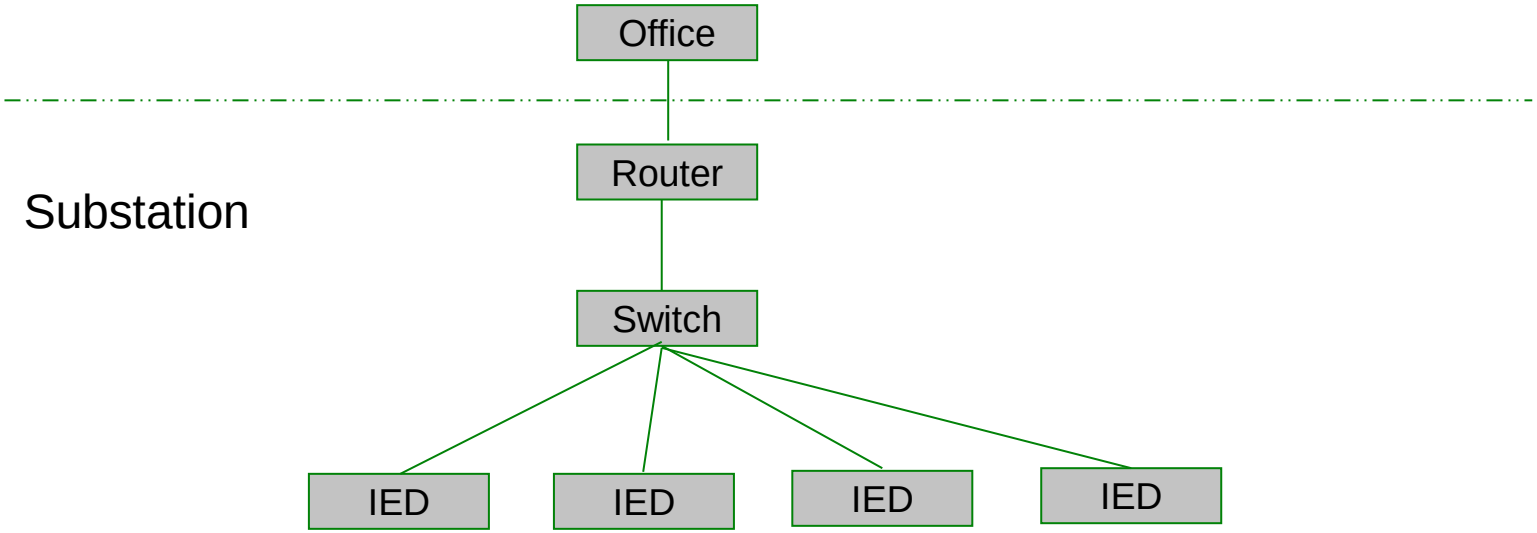
Reliability of network - Enterprise



Network types - Engineering

- Used by Engineering to access IED’s
  - Events
  - Load data
  - Settings
- Typically can be the same as a office network
  - No need for redundant networks
    - If the network fails, you can wait for it to be repaired
  - Do need to use substation harden equipment
    - All equipment needs to be designed for the environment used.
  - These systems are design to handle interruptions
  - Routers are needed for security reasons
    - These devices are designed for providing security

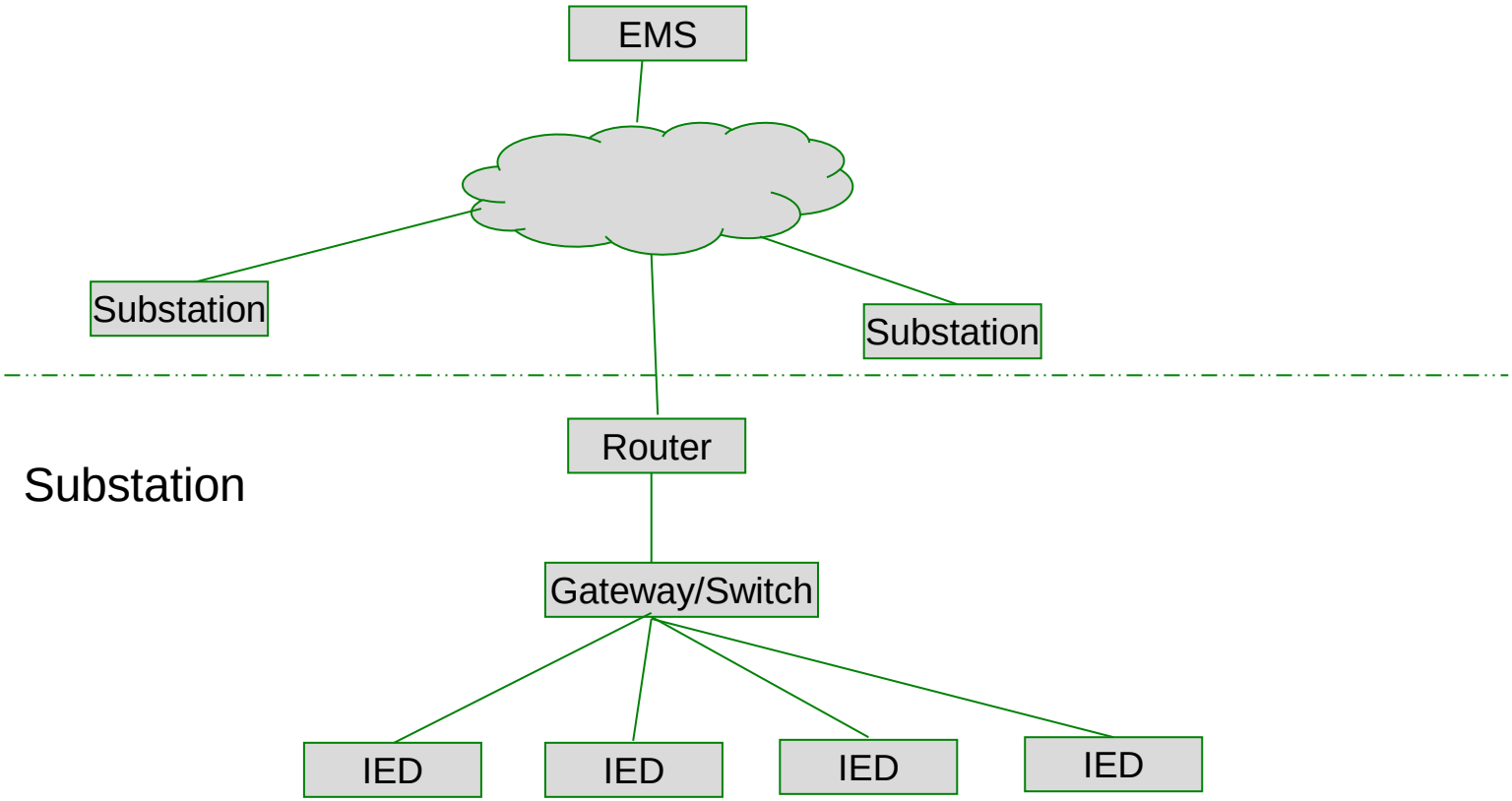
Reliability of network - Engineering



Network types - SCADA

- Used to provide data to remote control center
  - Should be separate from other networks
- Needs to have better reliability than office networks
  - Can accept some interruptions
    - Most systems have a fail/safe mode to account for interruptions in communications
  - Data needs to be secure
  - Data needs to be accurate

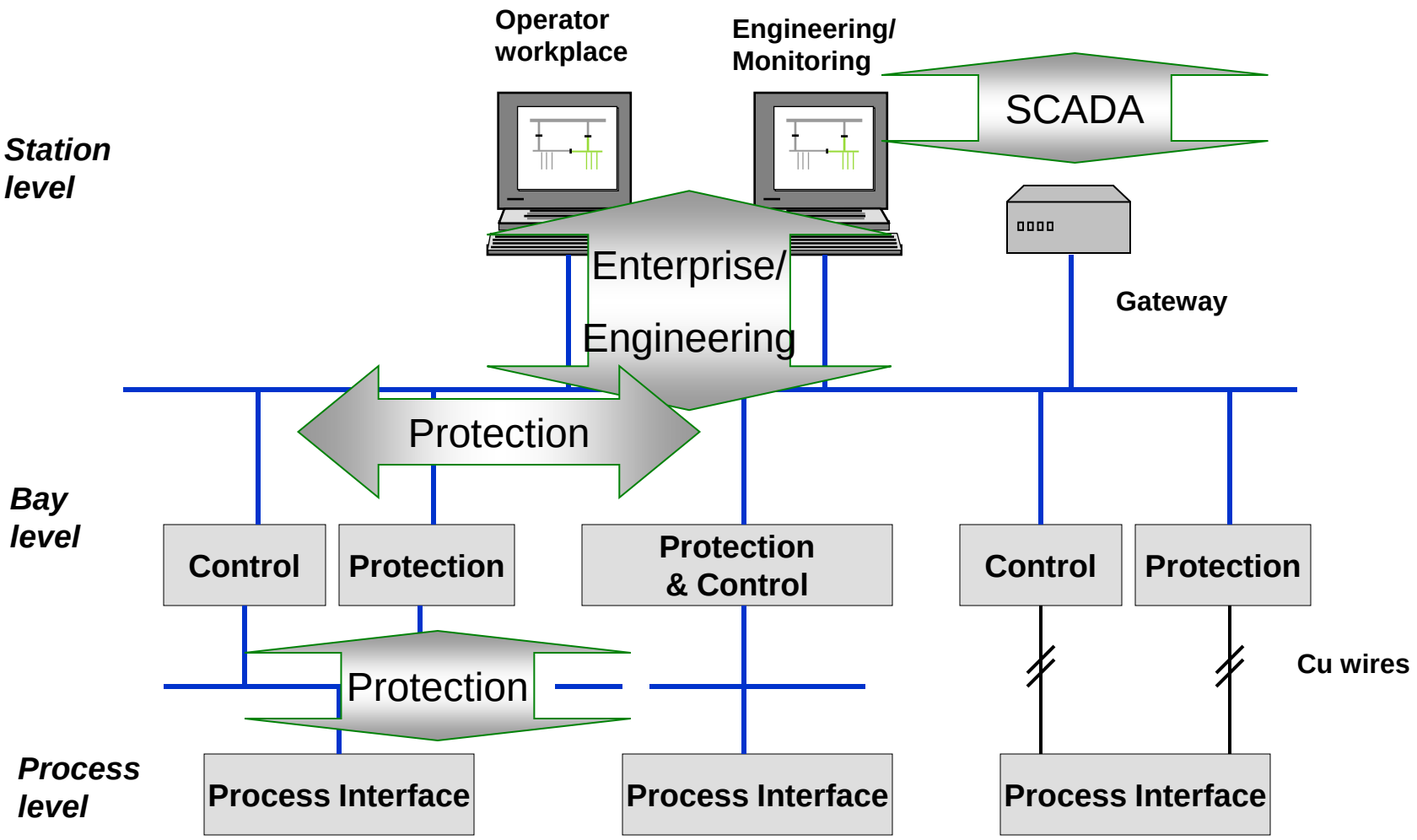
Reliability of network - SCADA



Network types - Protection

- Used to provide data between IED’s
- Should be separate from other networks
- Needs to have better reliability than office networks
  - Can not accept interruptions
  - Data needs to be secure
  - Data needs to be accurate
  - Needs to be deterministic
    - At least no large delays

Networks


Operator workplace
Engineering/ Monitoring
SCADA
Station level
Enterprise/ Engineering
Gateway
Protection
Bay level
Control
Protection
Protection & Control
Control
Protection
Protection
Cu wires
Process level
Process Interface
Process Interface
Process Interface

Reliability of network

- Network reliability = Data reliability
  - It is really data that is important
    - This is what drives the schemes
  - But networks affect the data
    - Network design affects the reliability
      - A poor design can make a network unreliable
    - Network parameters can also affect data reliability
      - Using the network parameters can assure data timeliness
      - Can assure the data gets to where it is needed

Reliability of network

Define a network structure

- Are you interfacing with Enterprise systems
- Are you providing SCADA data
- Are you doing protection over the network
  - Distribution protection
  - Transmission protection
- Are remote sites part of the protection

These questions will help determine the type of network that is needed.

Reliability of network - Enterprise

- Typically can be the same as a typical office network
  - No need for redundant networks
    - If the network fails, you can wait for it to be repaired
  - No need for self healing networks.
    - These systems are design to handle interruptions
  - Routers are needed for security reasons
    - To protect the Enterprise system from incursions from the substation

Reliability of network - Engineering

- Typically can be the same as a typical office network
  - No need for redundant networks
    - If the network fails, you can wait for it to be repaired
      - Regardless of what engineering says
  - No need for self healing networks.
    - These systems are design to handle interruptions
  - Routers are needed for security reasons
    - To protect the Enterprise system from incursions from the substation

If this network is used for sending settings to the IED, then it is recommended that this network be designed like a protection network.

Reliability of network - SCADA

- These can not be the same as a typical office network
  - They will need to be set up differently than what most IT people would expect
- The networks need to be reliable
  - If the network fails, you lose your remote alarm and control
  - Some delays on the network are acceptable
  - Network parameters will need to be modified to assure the reliability of SCADA messages
- These systems need to be designed to prevent interruptions
  - Use redundant networks
  - Use self healing networks
- Routers are needed for security reasons
  - These devices are designed for providing security
    - This is critical as a breach in security can affect both the substation and the SCADA systems

Reliability of network - Protection

- These can not be the same as a typical office network
  - They will need to be set up differently than what most IT people would expect
- The networks need to be reliable
  - If the network fails, you lose your protection
  - Delays on the network are unacceptable
  - Network parameters will need to be modified to assure the reliability of the Protection messages
- These systems need to be designed to prevent interruptions
  - Use redundant networks
  - Use self healing networks
- Routers are needed for security reasons (If the networks extends beyond the substation)
  - These devices are designed for providing security
    - This is critical as a breach in security can affect both the substation and the protection systems

Reliability of network – Protection - Distribution

- Distribution networks have different requirements from the Transmission networks
  - Protection tend to be designed to work without knowledge of other devices
    - If the network fails, you can revert back to the “old” schemes
  - Automation Schemes will become unavailable
    - Electrical system recovery will be lost

Reliability of network – Protection - Transmission

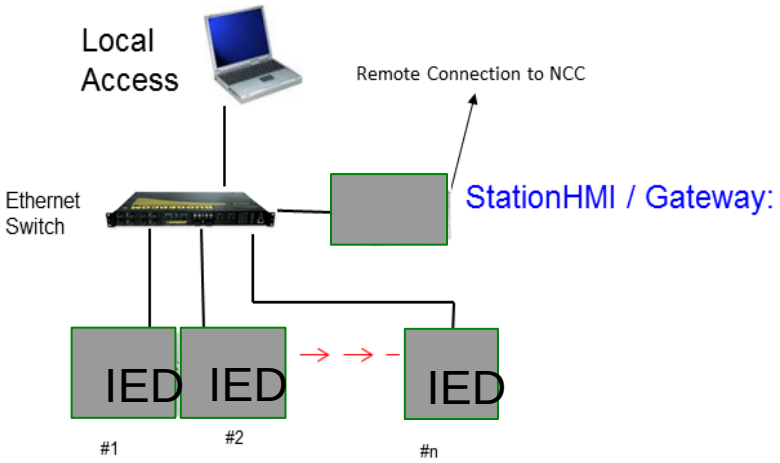
- Transmission networks have very unique requirements for networks
  - Protection schemes need information from other devices to work properly
    - If the network fails, the protection scheme is compromised
  - Data integrity is critical
    - Any excessive delay can cause the system to operate improperly

Reliability of network - Design

- Network Design
  - Star
  - Daisy
  - Channel Switching
  - Rapid Spanning Tree Protocol (RSTP)
  - High-availability Seamless Redundancy (HSR)
  - Parallel Redundancy Protocol (PRP)

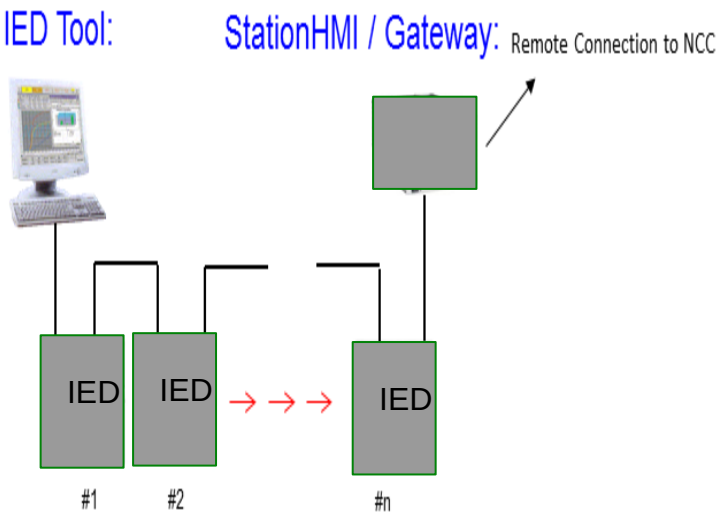
- Network Layout
  - Creating Separate Networks for Applications

Reliability of network – Star Topology



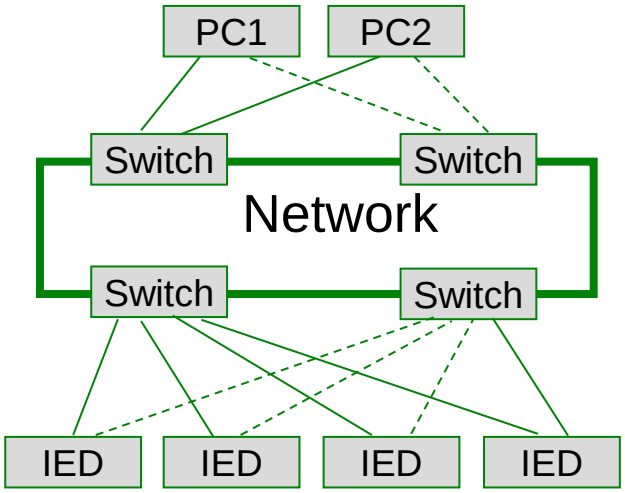
- Operation Mode
  - 1 Port active
  - Data is sent via one link
- Advantage
  - IEDs are not active part of the network
  - Simple design
    - Easy to Implement
    - Easy to troubleshoot
  - Failure of one IED does not affect the rest of the network.
- Disadvantage
  - Single point of failure
    - No switchover capabilities
  - No network redundancy, IEDs have to be on the same network

Reliability of network – Daisy Chain Topology



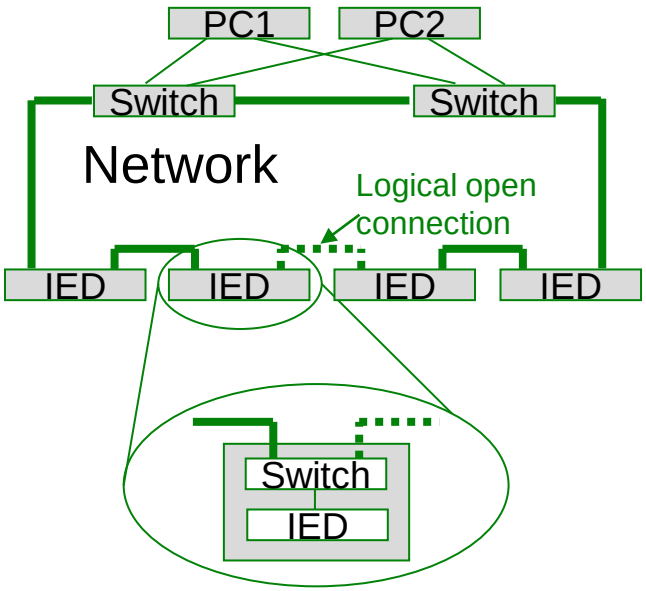
- Operation Mode
  - 2 Ports active
  - IEDs pass messages through to the next device
  - IEDS an active part of the network.
- Advantage
  - No need for routers/switches
- Disadvantage
  - No switch-over
  - Failure on one IED breaks the network
  - No network redundancy, IEDs have to be on the same network
  - Each IED has to handle multiple messages.
    - Can cause processing delays

Channel Switching Method
Principle



- Operation Mode
  - 1 Port active
  - 1 Port monitored passive (only link to switch is monitored)
  - Switch over time approx. 10ms
- Advantage
  - IEDs are not active part of the network
  - Failure of one device/link does not break the communications
- Disadvantage
  - Slow switch-over performance
  - Messages can be lost during switch-over
  - No network redundancy, IEDs have to be on the same network

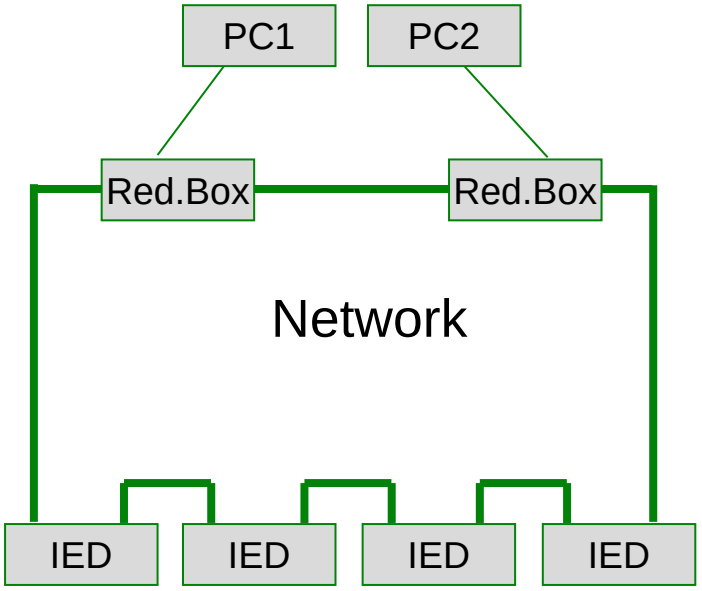
Integrated Ethernet Switch with RSTP
Principle



- Operation Mode
  - 2 ports active
  - RSTP protocol for ring redundancy
  - Recovery time typically 100ms (depends on the number of nodes and type of failure)
- Advantage
  - Low-cost
- Disadvantage
  - Slow recovery performance
  - Messages can be lost during recovering phase
  - No network redundancy
  - IEDs are active part of the network
    - Disconnecting, power-off IEDs disturbs or interrupts the network
  - Transmission delay by each “hop” (each IED)
  - Each IED has to handle multiple messages.
    - Can cause processing delays

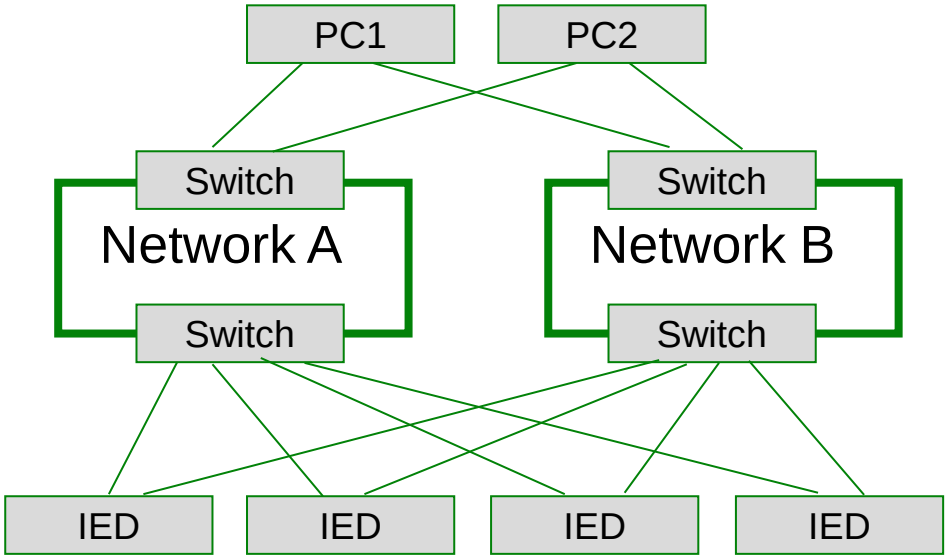
Integrated Ethernet Switch with High availability Seamless Redundancy

Principle



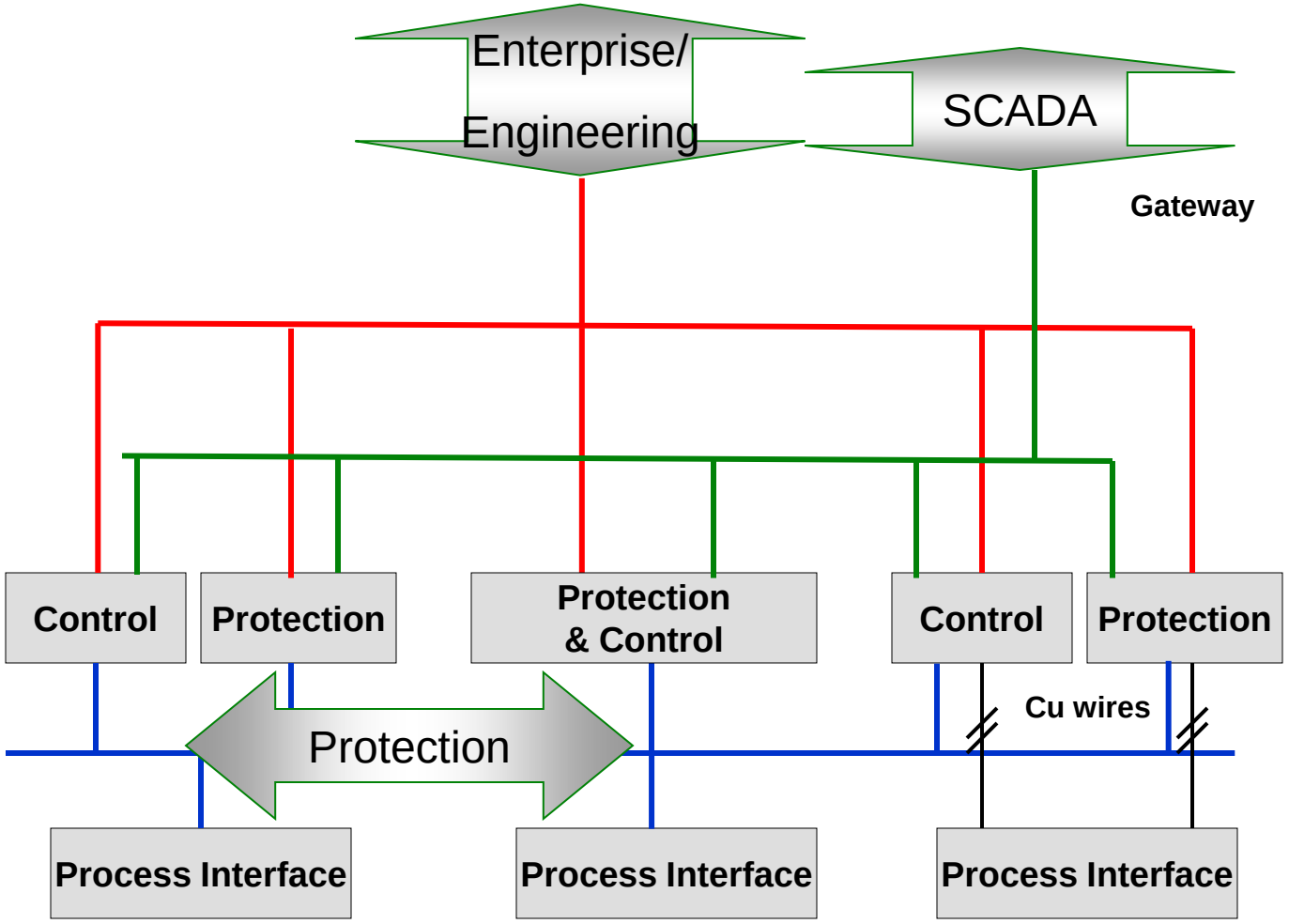
- Operation Mode
  - 2 ports active
  - HSR protocol for ring redundancy
  - Switch over time 0ms
  - Messages are sent in both direction at the same time
    - Second message is not used
    - Message is removed by sending device
- Advantage
  - Low-cost
  - No recovery time
  - No messages are lost
- Disadvantage
  - No network redundancy
  - IEDs are active part of the network
    - Disconnecting, power-off IEDs disturbs or interrupts the network
  - Transmission delay by each “hop” (each IED)
  - An Auxiliary device maybe needed (Redbox)

Parallel Redundancy Protocol (PRP)
Principle

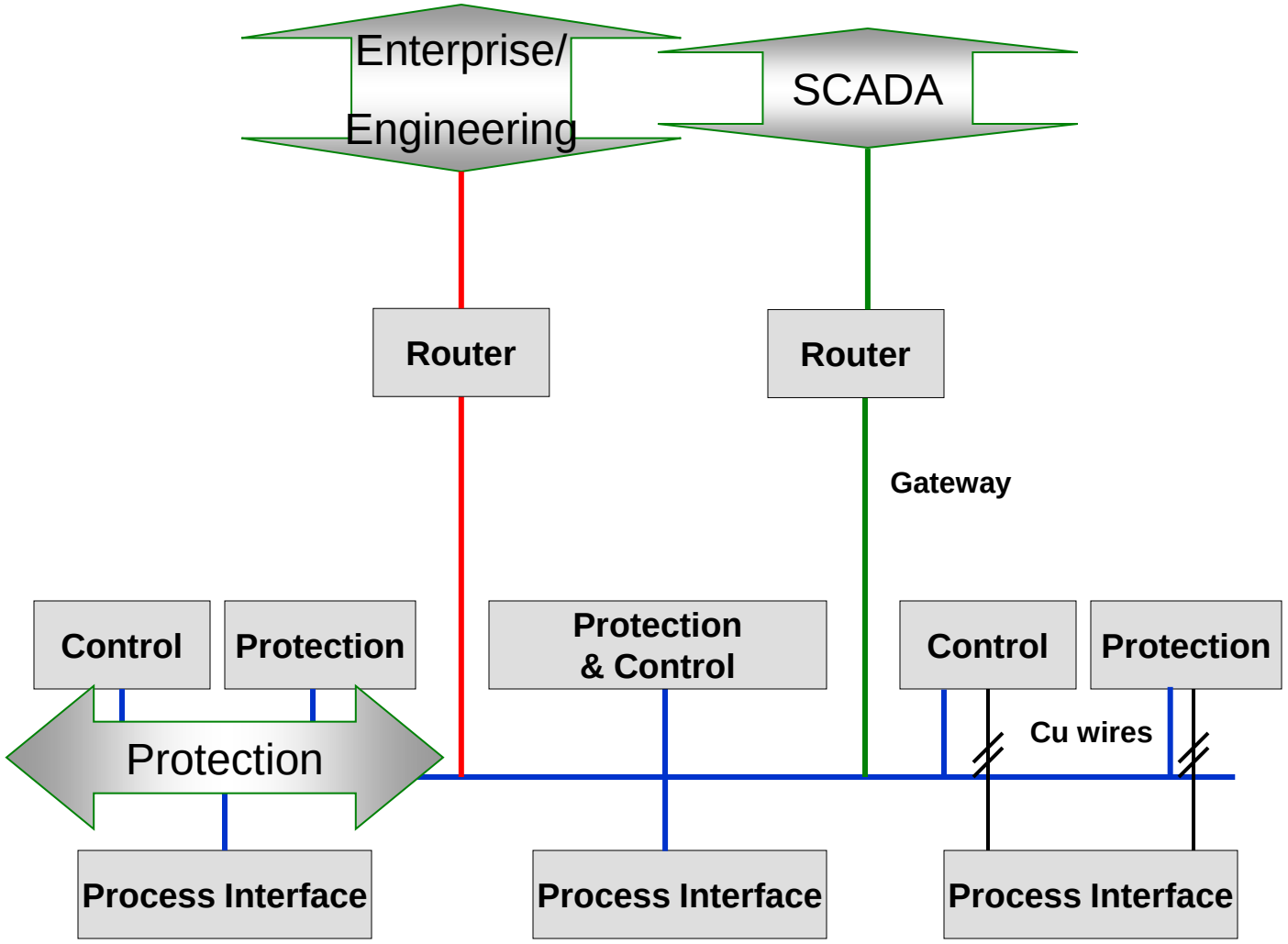


- Operation Mode
  - 2 Ports active
  - Messages are sent / received simultaneously on both ports
    - Second message is not used
    - Message is removed by sending device
  - Switch over time 0ms
- Advantages
  - No recovery time
  - No messages are lost
  - Network redundancy (Network A and B)
  - IEDs are not active part of the network
  - Standard according IEC 61850-8-1/9-2 Edition 2
- Disadvantages
  - Potentially Higher cost

Network – Ideal World



Network – Reality



Network - Reality

- Potential large amount of data
  - During Fault condition
  - Uploads/downloads from Enterprise systems
  - SCADA data
  - Most networks can handle this type of traffic
    - Some IED’s may not be able to
- Security risks
  - Unauthorized access
    - Data mining
    - Control
    - Viruses

These can be mitigated with the proper settings and hardware

Parameter Setting

- Parameters
  - Proper use can make the network more efficient
  - VLAN’s
    - Used to limit traffic to IED
  - Priority
- Security Risks
  - Use of routers
  - Encryption
  - Password rules
  - Work with your IT folks

Market Requirements Have Been Driving …

- Cost reduction in design, construction and operation
- Improved power system reliability and safety
- Safeguarding of investments
- A global, open standard
- Fit all types and sizes of substations and architectures

Contact information

If you have further questions , please contact me at:

PRESENTER	Jim Bougie
COMPANY	ABB
CONTACT PHONE	(414) 378-2763
CONTACT E-MAIL	james.bougie@us.abb.com