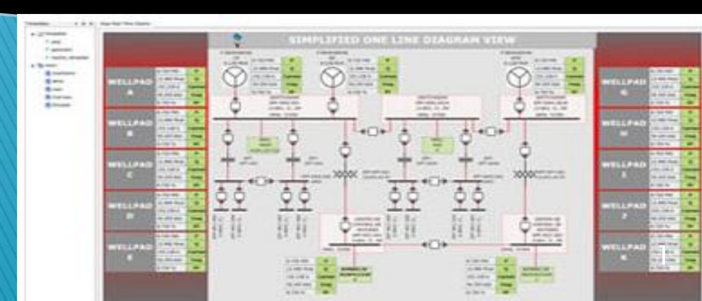
SCADA in electrical power delivery

Maxwell Dondo PhD PEng SMIEEE



Outline

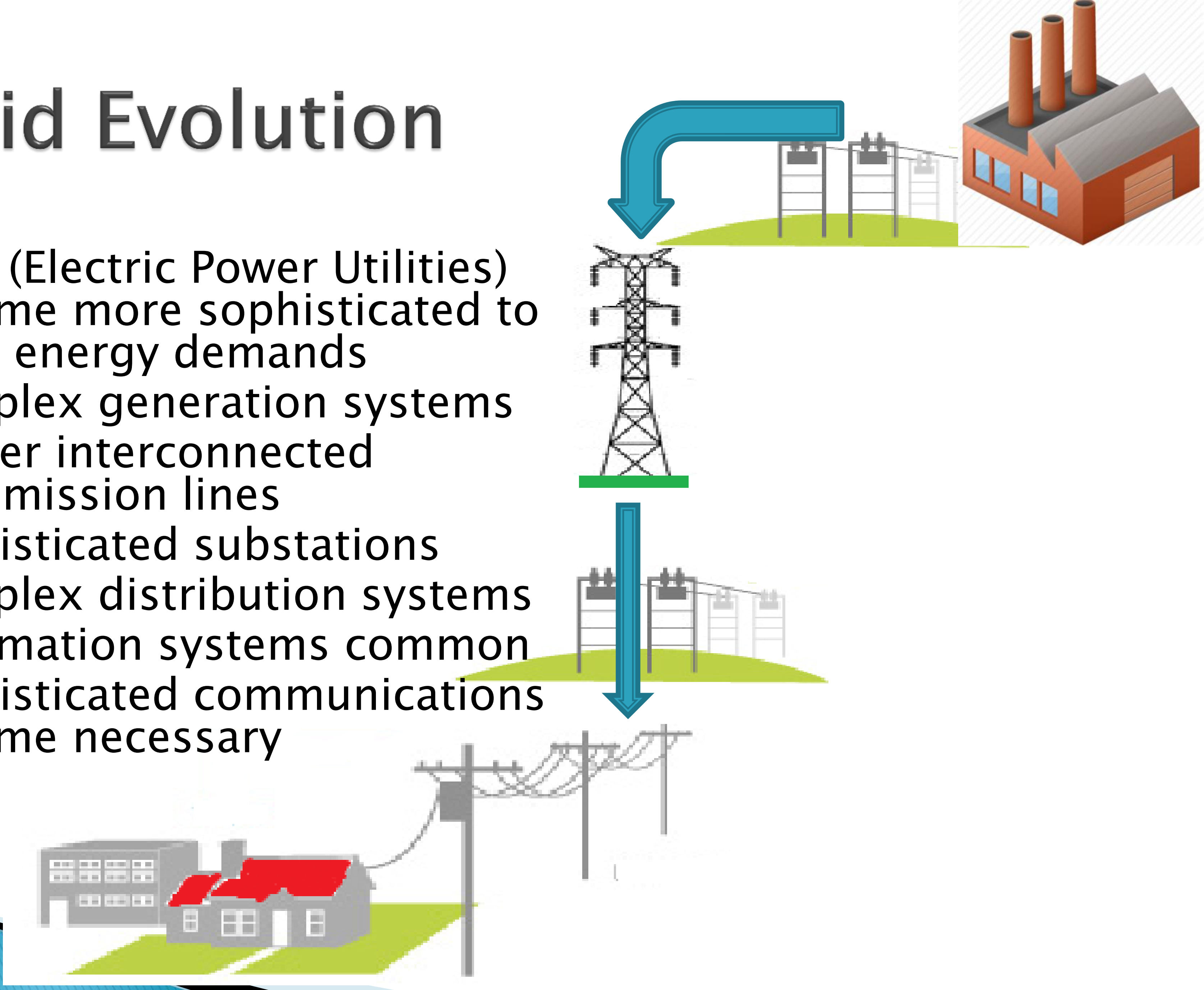
- Evolution of grid automation
- SCADA introduction
- SCADA Components
- Smart Grid
- SCADA Security

Grid Evolution

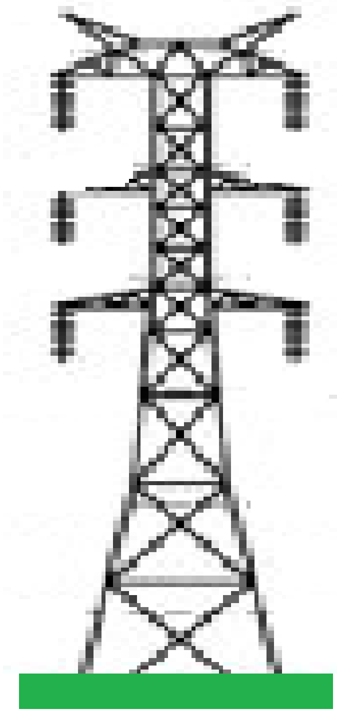
- Traditionally power delivery was unsophisticated
  - Generation localised around communities
  - Simple consumption (e.g. lights)
  - Simple communication with consumer
  - Consumer billed monthly
- System relied on consumer phone calls for fault notifications
- Ground crews dispatched to fix problems
- Time consuming process

Grid Evolution

- EPUs (Electric Power Utilities) became more sophisticated to meet energy demands
- Complex generation systems
- Longer interconnected transmission lines
- Sophisticated substations
- Complex distribution systems
- Automation systems common
- Sophisticated communications became necessary



Morden Electric Grid



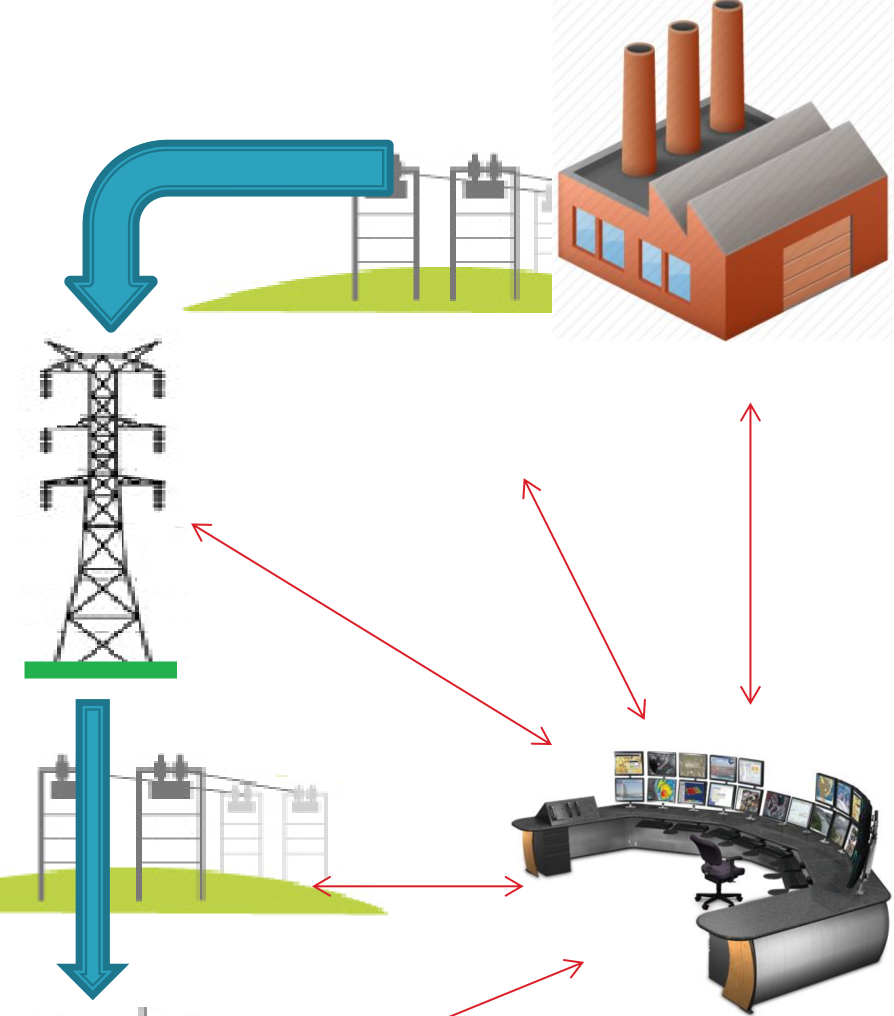
- Generation (usually 25kV or less)
  - Thermal
  - Hydro
  - Nuclear
  - “Green” Sources
- Transmission Lines
  - AC or DC
  - Transmit power at high voltage over long distances
  - High voltage, low current to reduce losses e.g. 735kV for James Bay transmission lines.

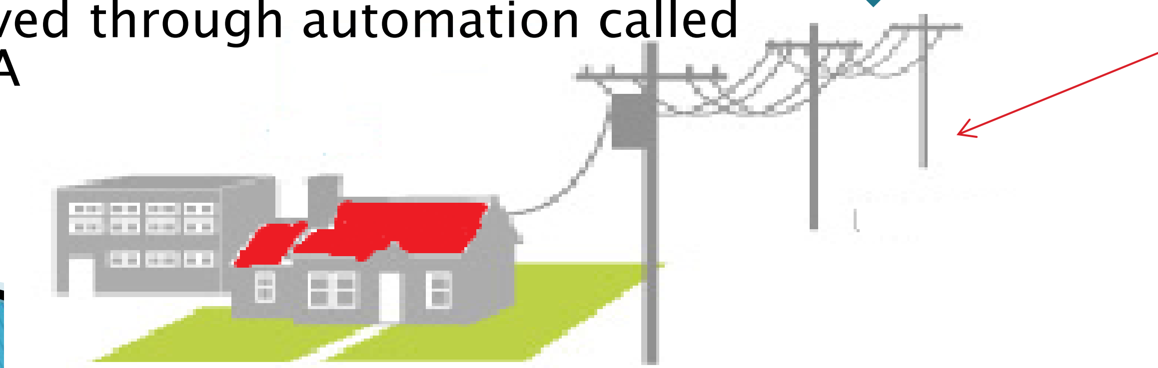
Morden Grid: Substations

- Substations ordinarily contain
  - Transformers step up/down voltages for transmission or distribution e.g. Distribution substation: 115kV/27.6kV
  - Instrument transformers (CTs/VTs), meters
  - Circuit breakers, switches, isolators, relays
- Substations are capable of local control and monitoring
- Substation can be of different varieties (e.g. simple switching station or very sophisticated distribution substation)

Grid Automation

- Grid evolved
  - from manned substations to remotely monitored and controlled system
  - from electromechanical systems to dial-up system
  - from unsophisticated one-way communication to two-way communication
- Automation became a requirement
- Regulatory reporting requirement
- Automation became integrated with preventative/predictive maintenance
- Need computers to process grid's operational and non operational data
- Achieved through automation called SCADA





SCADA Definition

- A complex computer based system that uses modern applications to analyse the electric power grid system to acquire data, monitor and control facilities and processes.
- SCADA applications can support dispatchers, operators, engineers, managers, etc. with tools to predict, control, visualize, optimise, and automate the EPU.

Summary of SCADA History

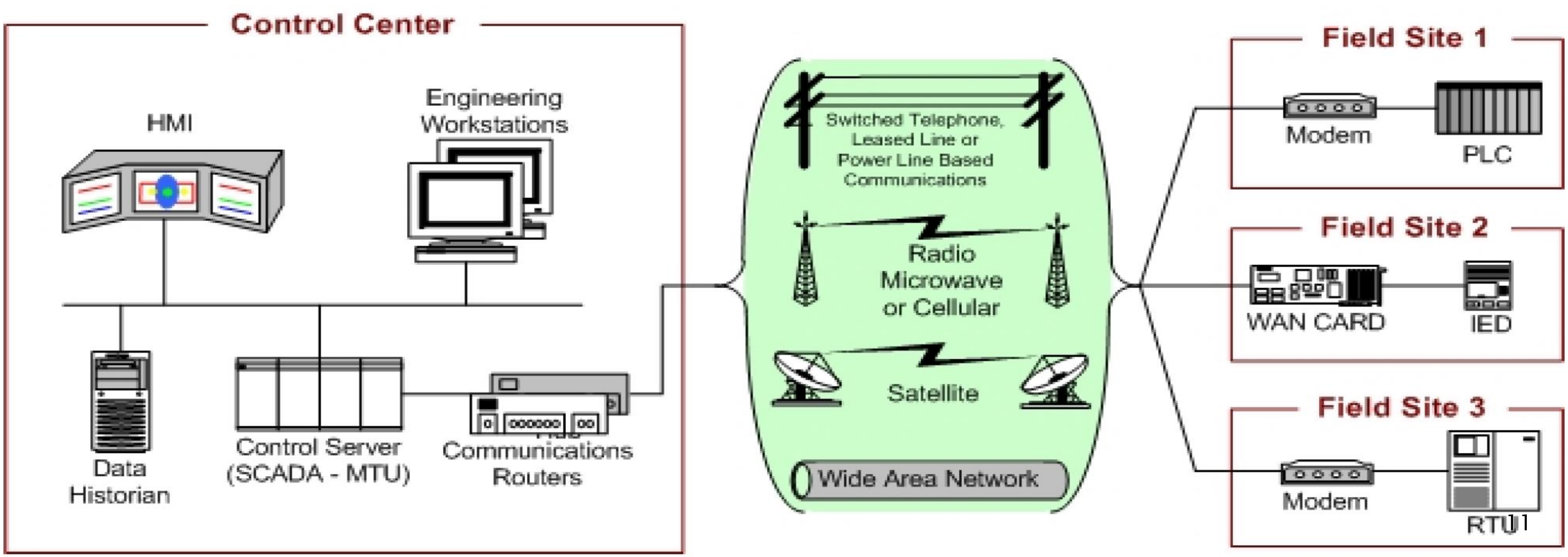
- Originally EPUs used electro-mechanical automation
- Dial-up modems used for remote access
- In 1970s computer-based SCADA commenced
- Suppliers (e.g. IBM, Siemens, GE) supplied complete proprietary systems
- More advanced with client-server computers
- Advanced functions became common (e.g. EMS. DMS, load forecasting, dispatch, protection engineering, regulatory reporting, etc)
- Communication link evolved from noisy narrow bandwidth telephone lines to SONET, Microwave, radio, power line carrier, cellular networks

Traditional SCADA Components

- SCADA Master Terminal Unit (MTU): The server that acts as SCADA system
- RTU (remote terminal unit) : remote telemetry data acquisition units located at remote stations
- IED (intelligent electronic devices) smart sensors/actuators with intelligence to acquire data, process it, and communicate
- HMI (human-machine interface) : software to provide for visualisation and interaction with SCADA

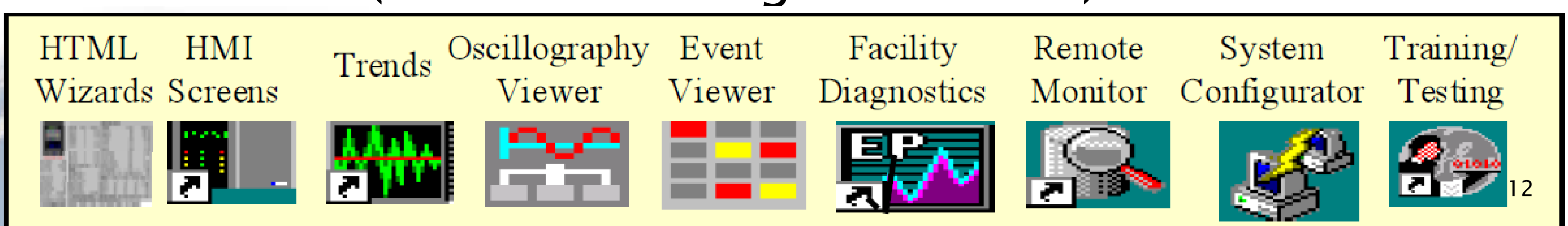
Overall SCADA System architecture

- Can be broken down into 3 categories
- NIST representation of SCADA system
  - Control Center
  - Programmable Logic Controllers(PLCs), Remote Terminal Units (RTUs), IEDs
  - Communications Network



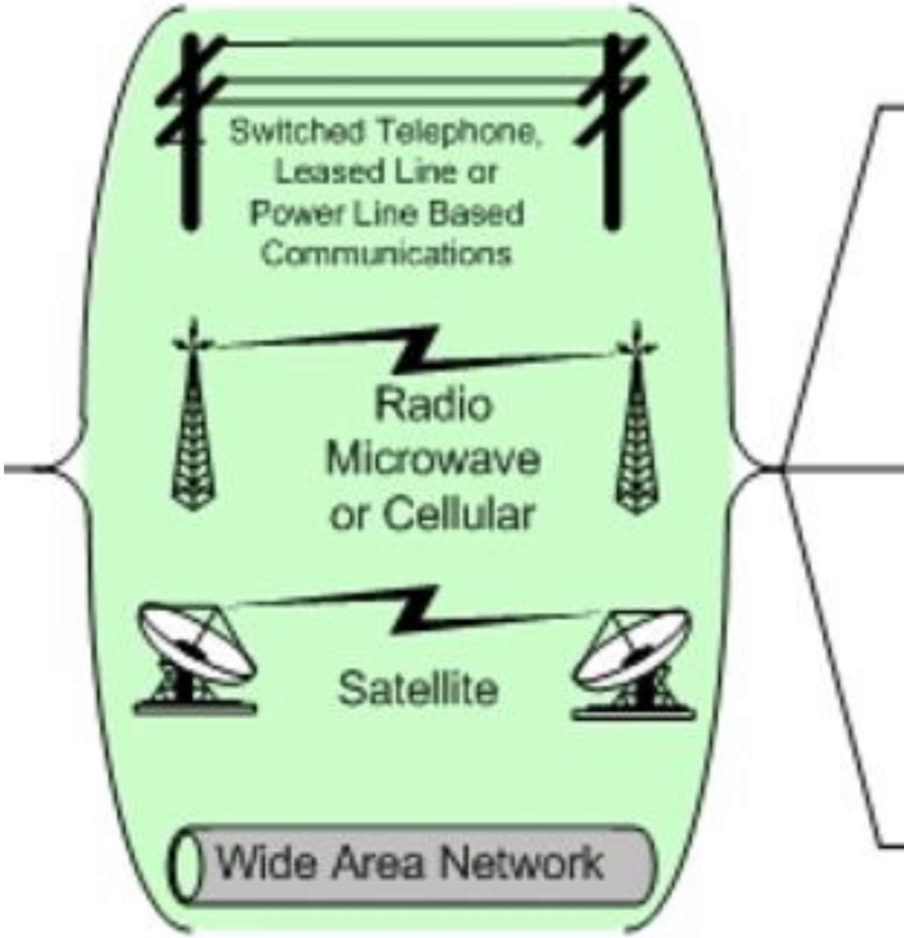
Control Center

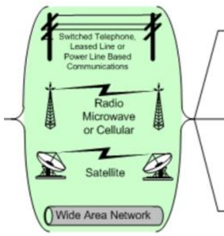
- Provides for real-time grid management
- SCADA Server
  - Also known as the MTU (master terminal unit)
- HMI for visualisation and human interaction
- Programming/Engineering workstations
- Data historian, a database storage for operational activities
- Control server, hosts software to communicate with lower level control devices
- Communication routers
- Could be connected to other regional control centers (desired for large networks)



Communication Link

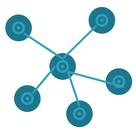
- Phone line/leased line, power line carrier
- Radio
- Cellular network
- Satellite
- Fibre optic



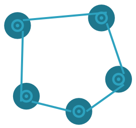


Communication topologies

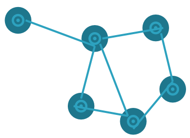
- Star



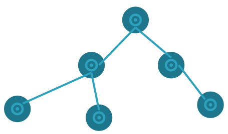
- Ring



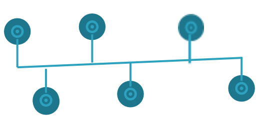
- Mesh



- Tree

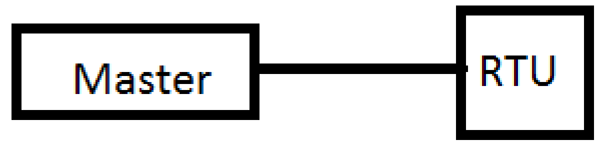


- Bus

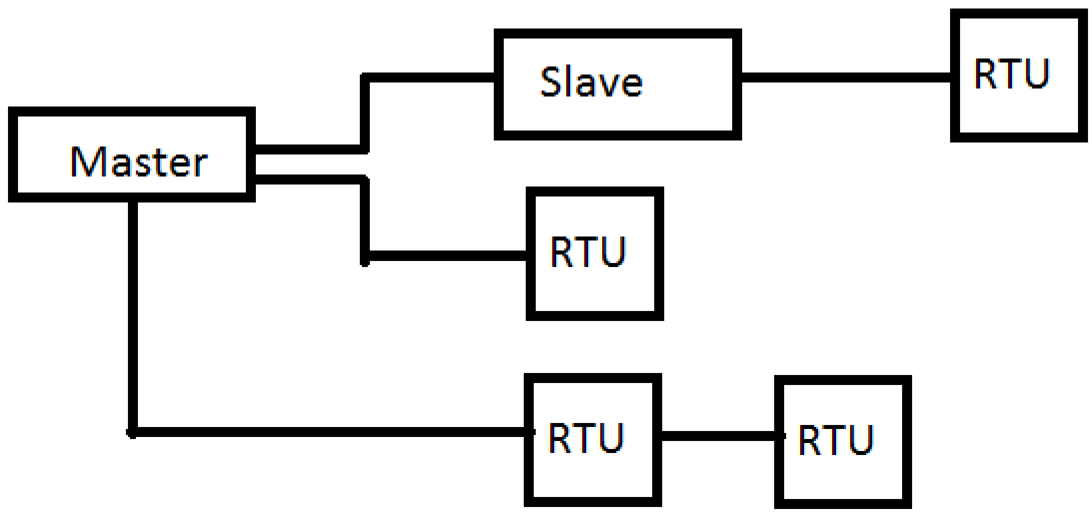


Implementation Examples

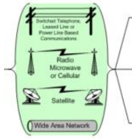
- Many possible topologies
- Direct connection



- Connection with slave

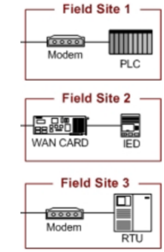


- Other. See IEEE C37.1



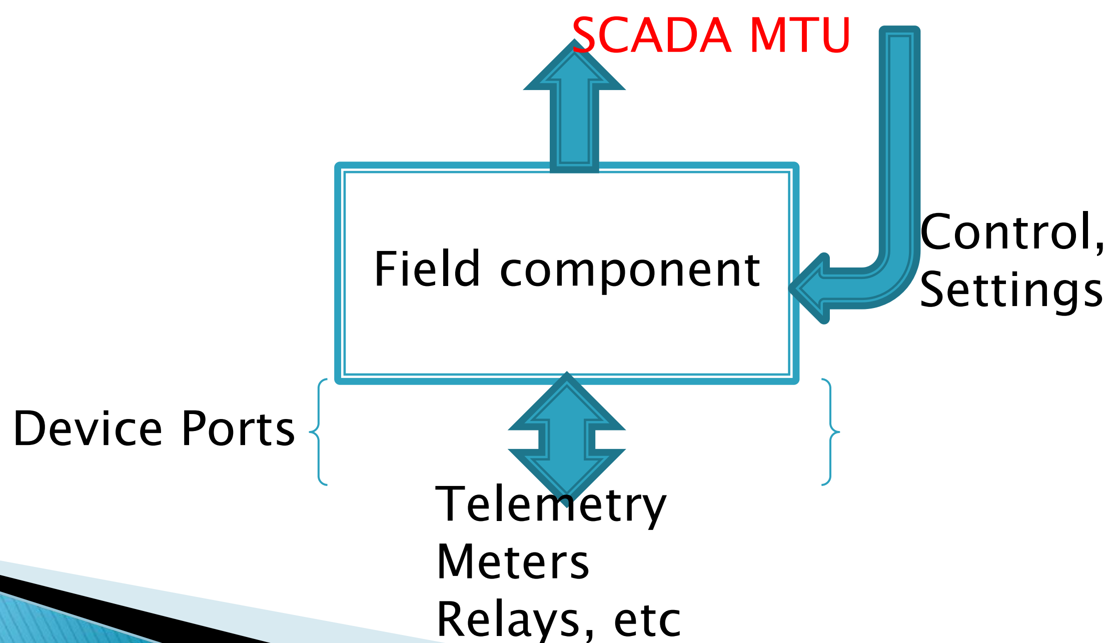
Protocols and standards

- Allow communications between devices
- MODBUS: master-slave application-layer protocol
  - Attackers with IP access can run Modbus client simulator to effect many types of attacks.
- DNP3 : Distributed Network Protocol is a set of open communication protocols
  - IEEE recommended for RTU to IED messages
  - Has no in-built security: Messages can be intercepted, modified and fabricated.
- IEC 60870 suite:
  - Substation control centre communication (IEC 60870-5-101/104)
  - Communication with protection equipment (IEC 60870-5-103)
  - IEC 62351 intends to implement security (end-to-end encryption; vendors reluctant to implement due to complexity)
- Other proprietary protocols

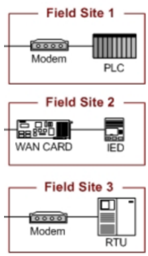


Field Components

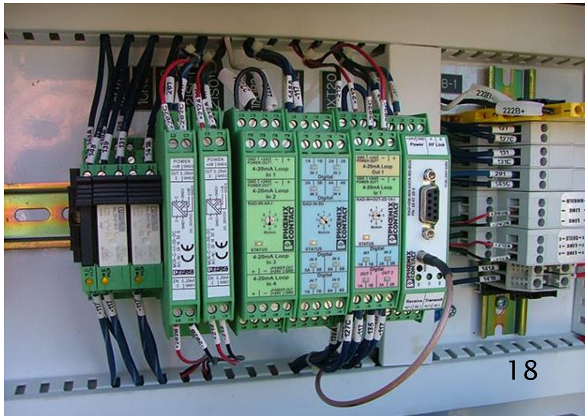
- Acquire telemetry, relay data from system
- Covert it to digital signals if necessary
- Send data to MTU or engineering stations
- Receive control, settings, resets from MTU



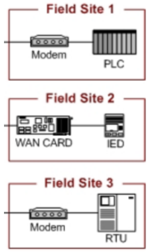
Field Components: RTU



- Reads status and alarms through relay and control circuit auxiliary contacts. Meter reading.
- Manual/remote control e.g. activate alarm. RTU control outputs connected to control relays
- No data storage
- Some PLCs equipped to be RTUs
- May aggregate IED data
- Either open standard or proprietary based
  - Modbus, DNP3, IEC 60870-5-101/104
- Serial communication
  - RS232, RS485

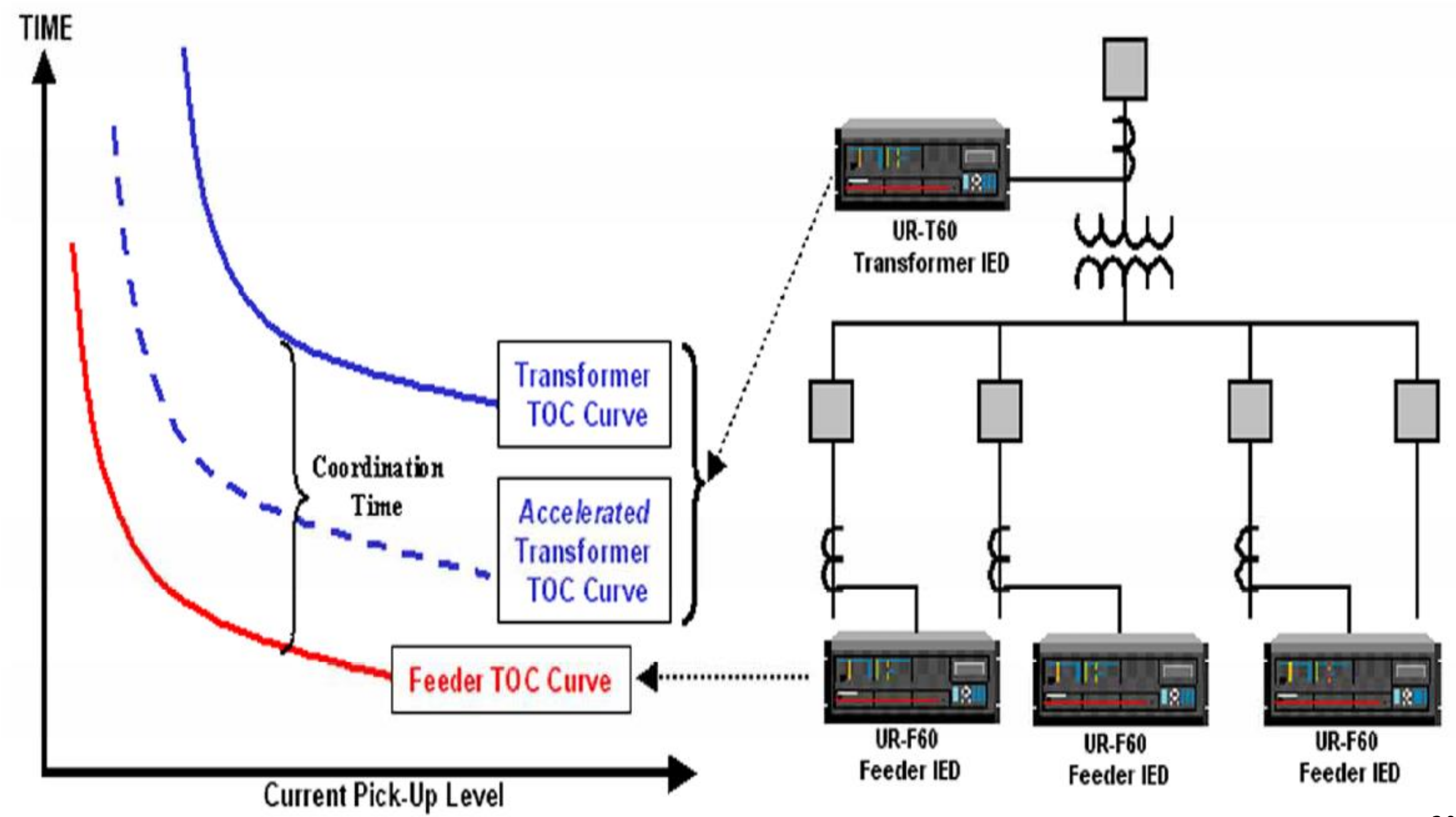


Field Components : IED



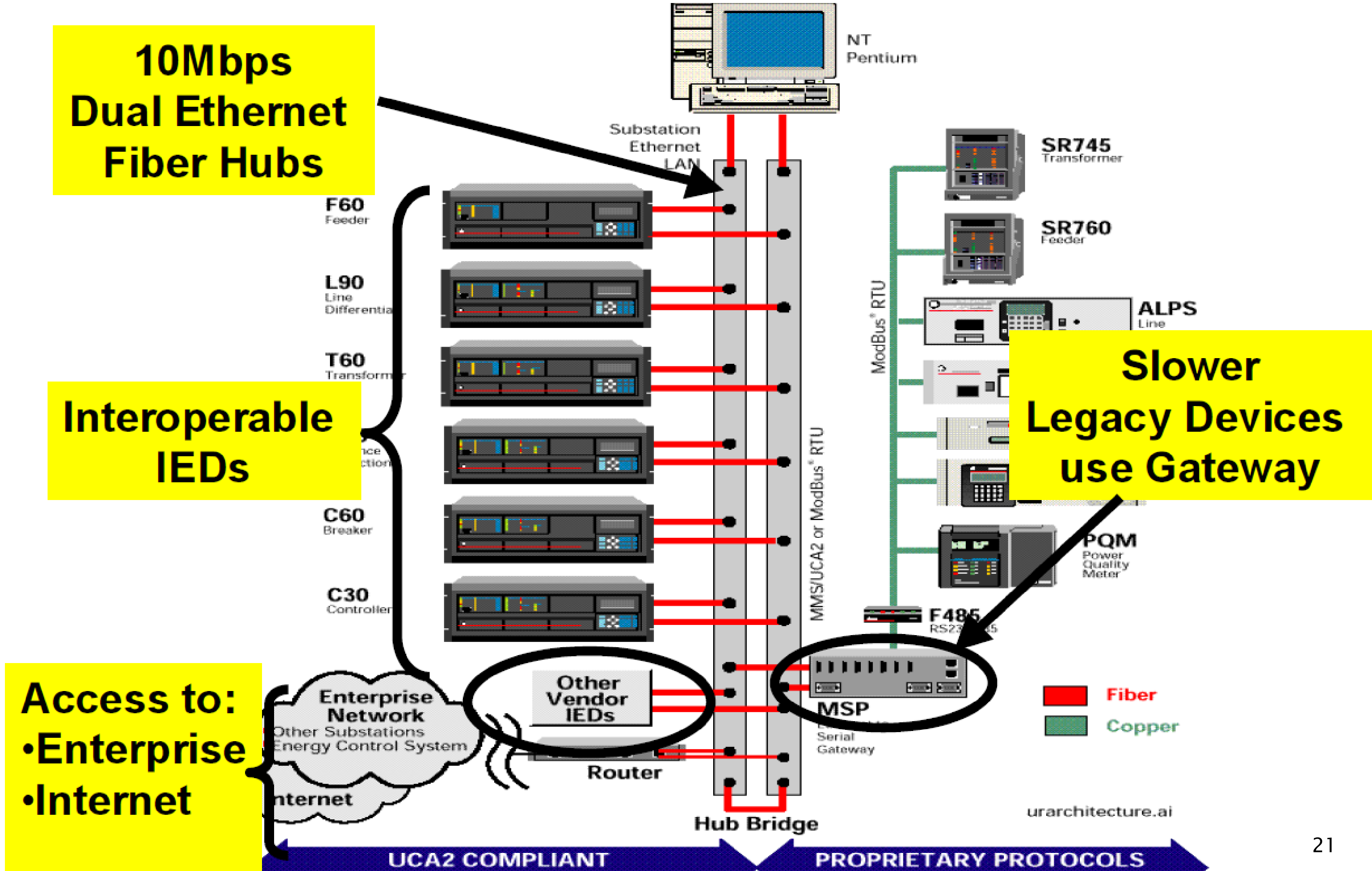
- Similar to RTU, is open or proprietary based
- Acquires data from electrical devices, e.g. relay or circuit breaker status, switch position.
- Reads meter data such as V, A, MW, MVAR. Some modern meters have IED capabilities, they can communicate their readings with RTU or MTU.
- Control functions include:
  - CB control, voltage regulators, recloser control.
- Newer substations only use modern IEDs
- IEDs can support horizontal communication

GE Example

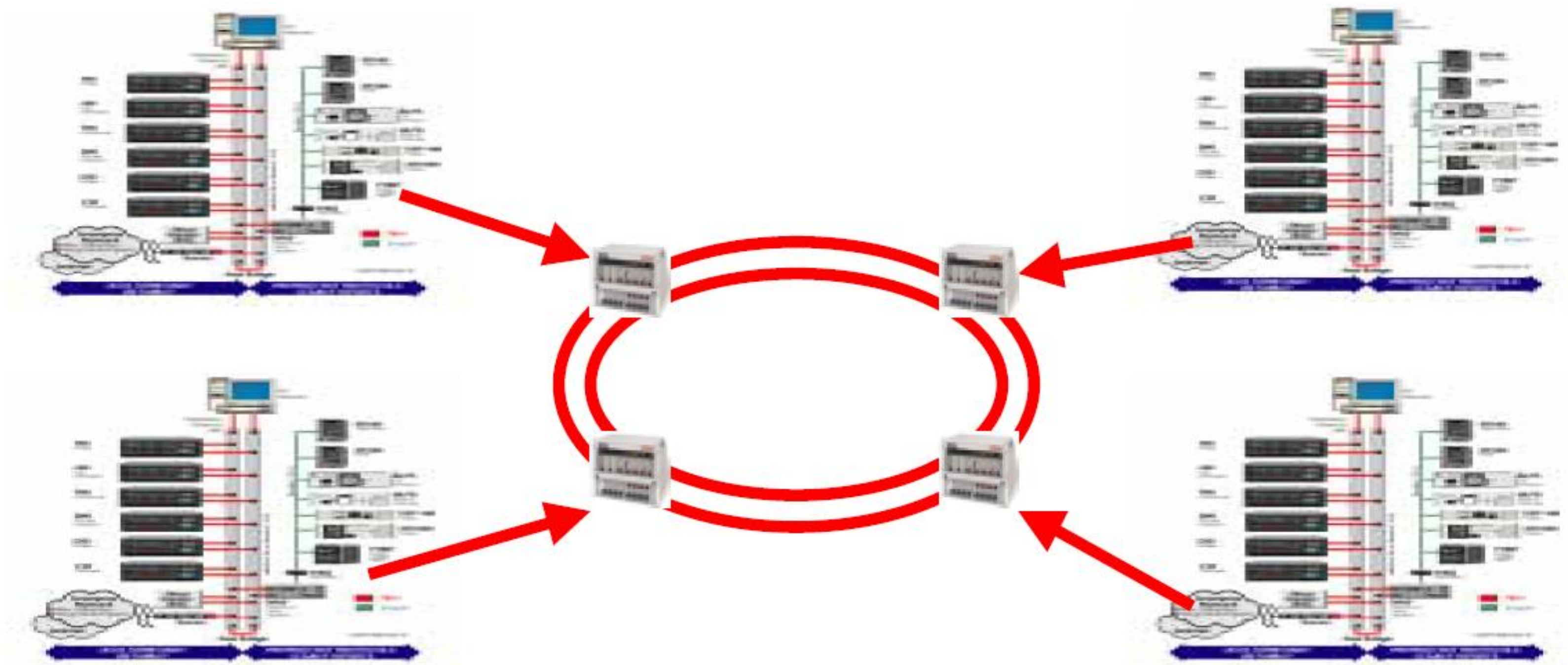


TIME
Coordination Time
Transformer TOC Curve
Accelerated Transformer TOC Curve
Feeder TOC Curve
Current Pick-Up Level
UR-T60
Transformer IED
UR-F60
Feeder IED
UR-F60
Feeder IED
UR-F60
Feeder IED

GE Example


10Mbps
Dual Ethernet
Fiber Hubs
Interoperable
IEDs
Access to:
•Enterprise
•Internet
Slower
Legacy Devices
use Gateway
NT
Pentium
Substation
Ethernet
LAN
F60
Feeder
L90
Line
T60
C60
Breaker
C30
SR745
Transformer
SR760
Feeder
ALPS
Line
PQM
Power
Quality
Meter
ModBus® RTU
MMS/UCA2 or ModBus® RTU
Other
Vendor
IEDs
Router
Enterprise
Network
Other Substations
Energy Control System
MSP
Serial
Gateway
Hub Bridge
Fiber
Copper
urarchitecture.ai
UCA2 COMPLIANT
PROPRIETARY PROTOCOLS

GE Example

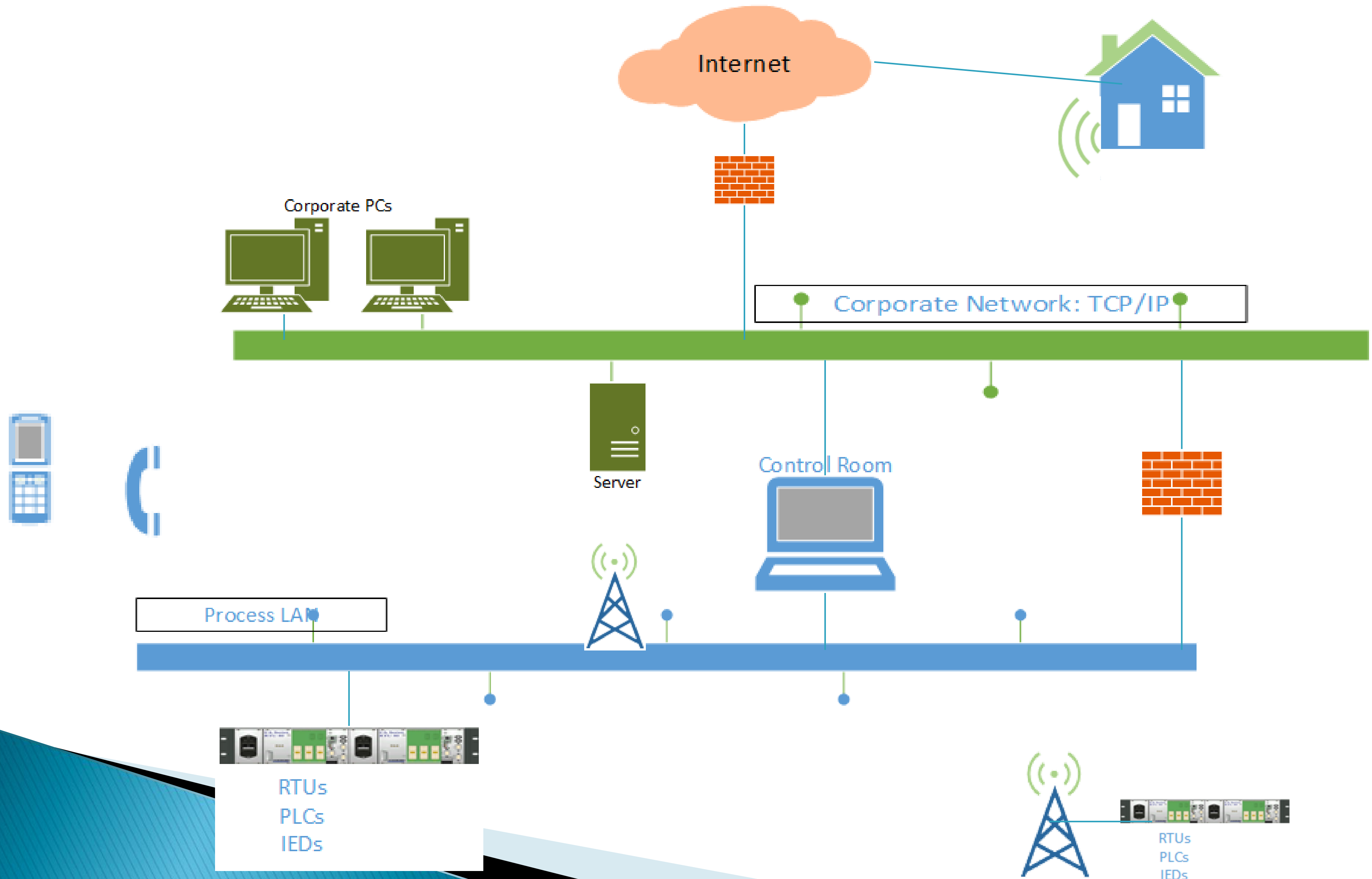


FSC

(Fiber Optic System Communications)

- SONET Technology: 51/155 Mbps
- Ethernet LAN 'Bridging' capability
- Creates single Ethernet WAN
- Redundant channels ensure reliability

SCADA and internet connection

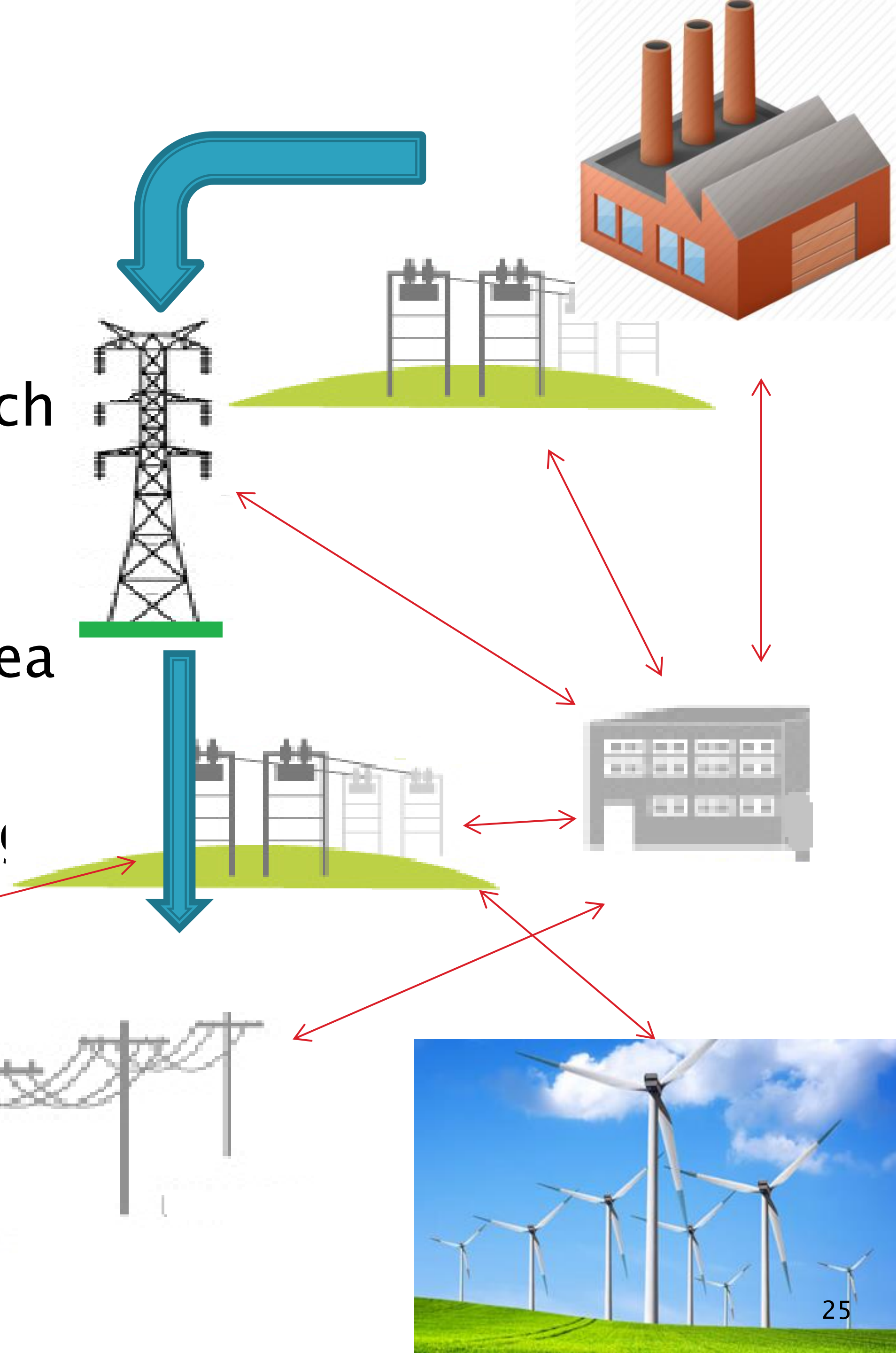


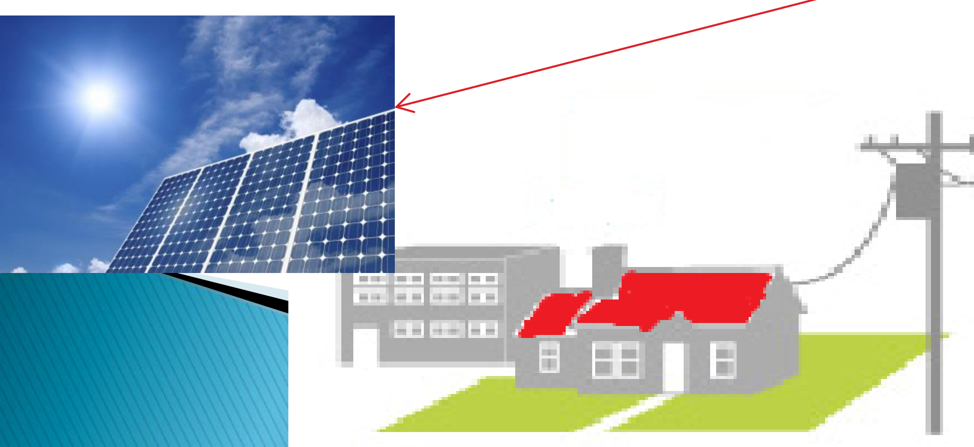
Smart Grid

- Concept of a fully automated power distribution system that can monitor and control all aspects of the system
- Ideally a smart grid provides voltage/power flow optimisation and self healing (after disruption)
- SCADA, WAMS, AMI provide and enable the "brains" of the smart grid concept
- SCADA makes real-time automated decisions to regulate voltages, optimal power flows, etc.

Smart Grid

- Supports sophisticated two-way communication
- Allows efficient power dispatch
- Easy to integrate with other sources e.g. green energy
- Supports smart metering
- Can coordinate with home area networks (HANs) for efficient consumption
- Supports efficient self-healing after faults



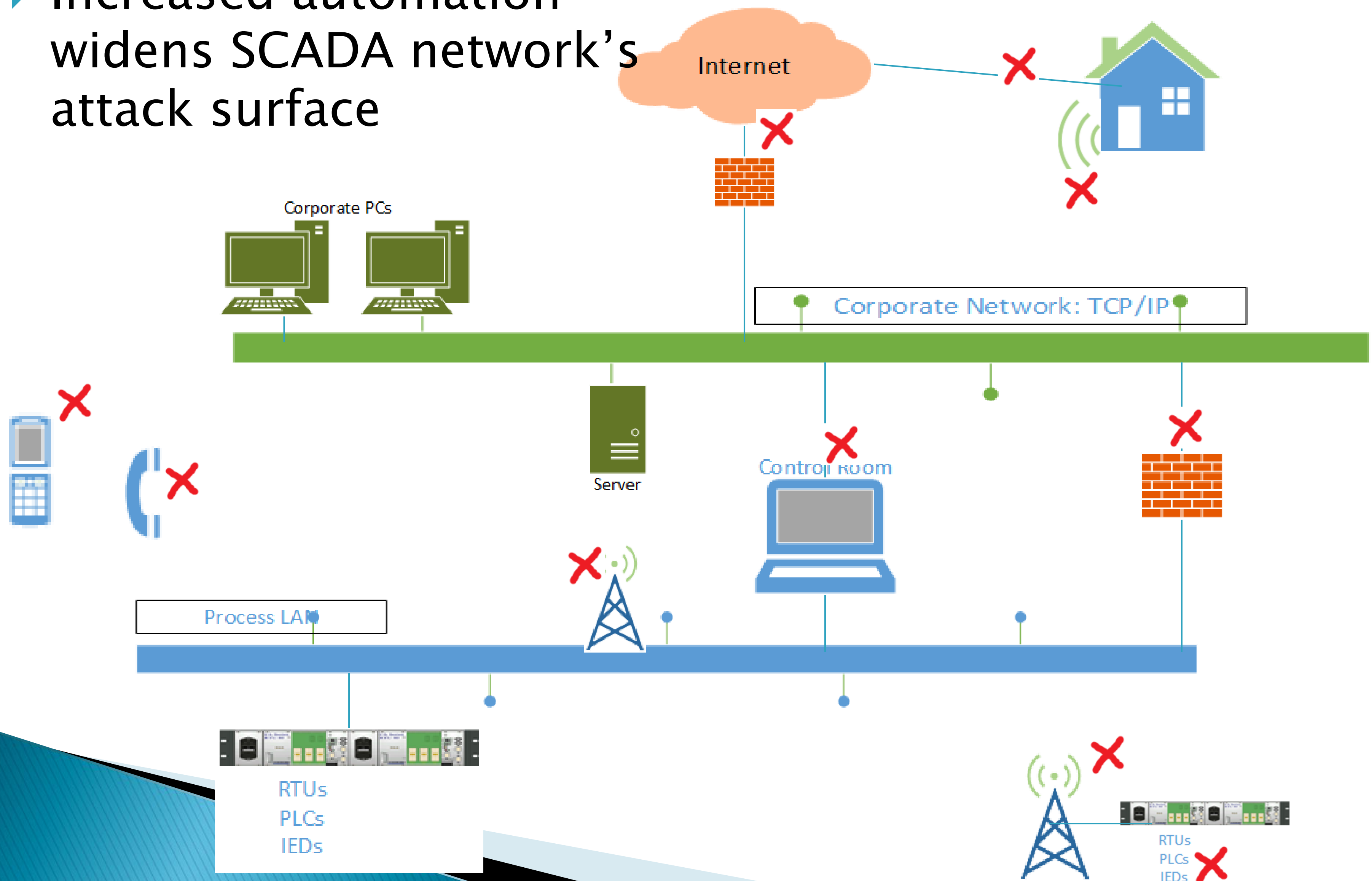


SCADA Security

- Traditionally isolated networks
- No security measures deemed necessary; security by obscurity
- Only threats were insiders and physical sabotage
- Modem war-dialing was also possible threat
- With interconnected EPU, SCADA is connected over wide area networks and internet
- That has exposed SCADA to attacks

SCADA Security Holes

- Increased automation widens SCADA network's attack surface



Typical SCADA threats (actors)

- Espionage
  - Spies (industrial and state actors)
  - Terrorists
- Script kiddies
- Insiders, e.g. disgruntled employees
- Criminal elements (blackmail)
- Business competitors
- Hacktivists (ideological activists)

SCADA Vulnerabilities

- Vulnerabilities are weaknesses in the cyber system that threats (actors) exploit to carry out attacks
- Examples of forms vulnerabilities:
  - Technical
    - Hardware
    - Software and protocol
    - Network
  - Policy

Vulnerability examples

- CVE-2015-1179: Allows remote attackers to inject arbitrary web script; found in Mango Automation systems
- CVE-2015-0981: Allows remote attackers to bypass authentication and read/write to arbitrary database fields via unspecified vectors.
- CVE-2015-0096 (MS15-018) : Stuxnet, a worm targeting ICSs such as SCADA.
- Other examples from 2014: CVE-2014-8652 , CVE-2014-5429
- GE Energy's XA/21: 2003 flaw responsible for alarm system failure at FirstEnergy's Akron, Ohio control center

Attack Examples

- Stuxnet: Intercepts and makes changes to data read from and written to a PLC
- Night Dragon : Suspected SCADA data exfiltration from Exxon, Shell and BP
- Others: Havex (Trojan targeting ICSs and SCADA), Blacken (Targets users of SCADA software Simplicity)
- Many others targeting the PCs used in SCADA.

Securing SCADA

- Define SCADA security networking policy
  - Access control
  - Identify all SCADA assets and their connectivity
  - Schedule regular vulnerability assessments
- User training and awareness (e.g. what to do when you pick up a USB stick in parking lot)
- Technical
  - Isolate SCADA from internet as much as possible
  - Encryption of data
  - Implement strict firewall rules between SCADA network and all other networks.
  - Perform anomaly detection

Securing SCADA

- Put in place effective policies
- Limit access to SCADA network; implement tight security access controls
- Use hardened hardware
- Patch regularly, don't use unpatched software or vulnerable systems
- Implement vendor security features (No defaults)
- Audit (include red teaming) SCADA IT systems for security holes

Summary

- SCADA systems enhance power delivery by providing grid situational awareness and control
- Delivers operational and non-operational data through a variety of communication methods
- SCADA is an important part of the Smart Grid
- SCADA system is traditionally insecure, security measures needed

References

- IEEE Standard for SCADA and Automation Systems C37.1, 2007
- IEC 61850 Communication networks and systems in substations
- Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security, NIST, 2007
- G. Clarke, and D. Reynders, Practical Modern SCADA Protocols, Elsevier 2004

Thank You

maxwell.dondo@drdc-rddc.gc.ca