Substation Automation Strategies for the Future

IEEE PES Meeting
Oak Brook, IL
January 28, 2015

by Ray Wright
NovaTech VP - Utility Marketing
ray.wright@novatechweb.com

NovaTech

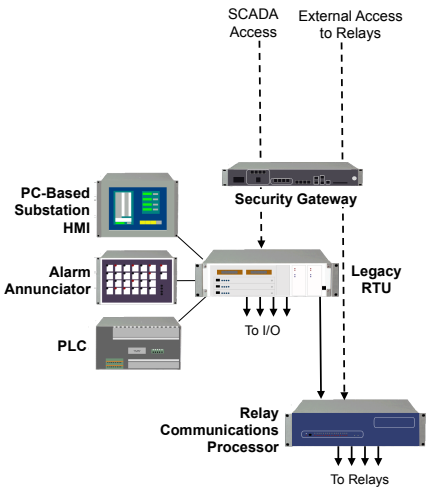
Substation Automation Strategies for the Future

- Box Consolidation
- Getting Data from IEDs Instead of from Hard-Wired I/O
- Expansion of Ethernet
  - More Ethernet Inside Substations
  - IEDs with Built-in Switches
  - Time Synchronization over Ethernet
- New Protocols
  - DNP3 "Secure Authentication"
  - IEC 61850
- Web-Based SCADA Instead of PC-Based SCADA
- Protection using 61850 Process Bus
  - Distributed Measurement, centralized protection

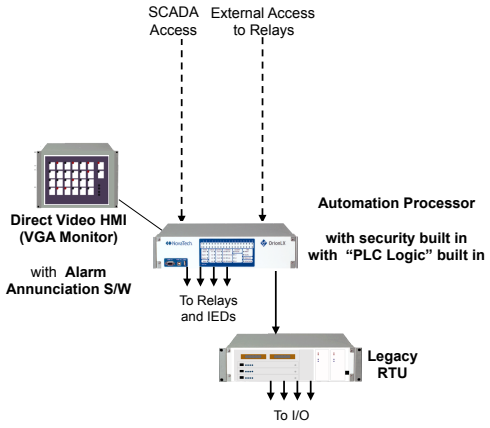
NovaTech

Box Consolidation

Legacy Approach



"Box Consolidation" Approach



Fewer boxes performing more functions

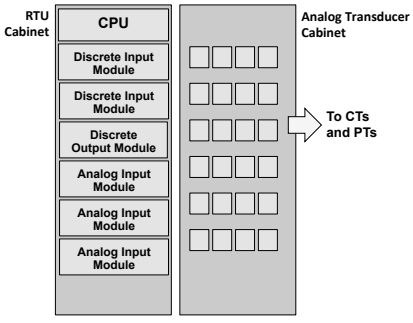
Reduce all costs

NovaTech

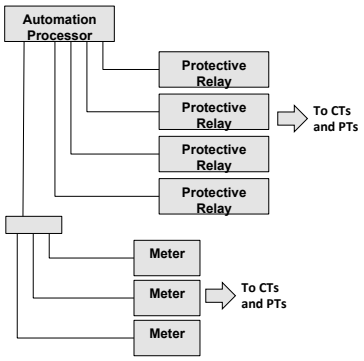
3

Getting Data from IEDs Instead of from Hard-Wired I/O

- Traditional RTU
  - Uses "hard-wired" I/O modules
  - Discrete I/O
    - Connected to breakers
    - Alarm contacts
  - Analog I/O
    - Connected to analog transducers



- "Smart" RTU
  - Minimal, if any, hard-wired I/O
  - Most "I/O" accessed through IEDs



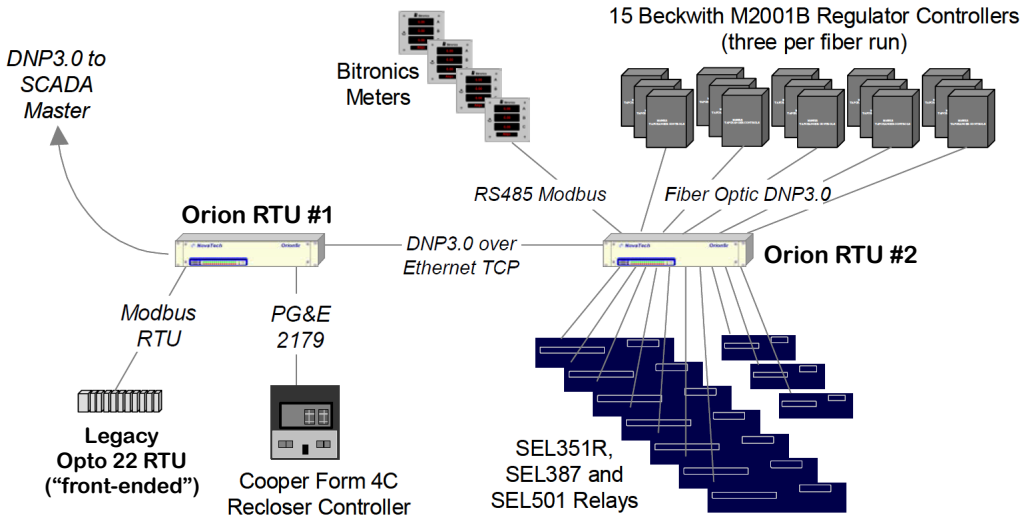
Reduce wiring and labor costs

NovaTech

4

Early "Smart RTU" Example

Wisconsin Public Service - 2004



NovaTech

5

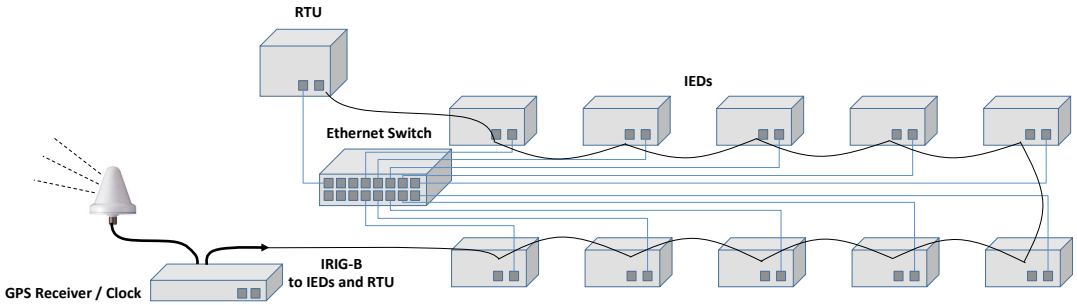
Expansion of Ethernet

- More Ethernet in Substations
- Time Synchronization over Ethernet
- IEDs with Built-in Switches

NovaTech

6

Time Synchronization over Ethernet



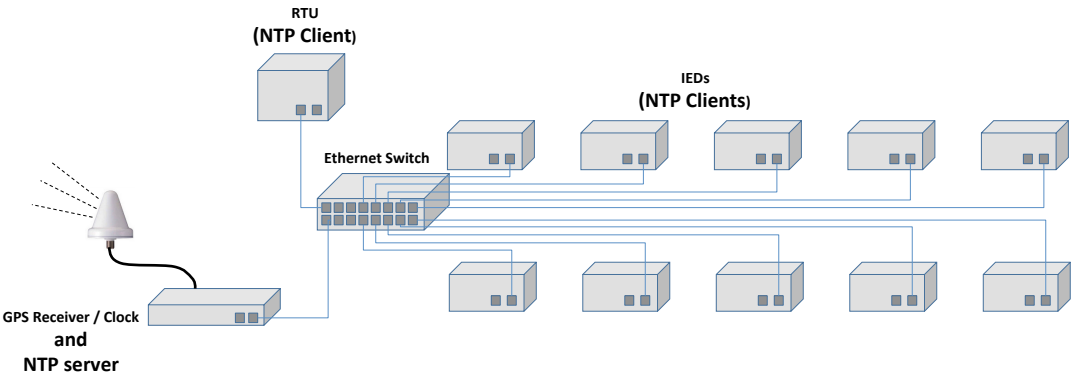
Traditional Approach

NovaTech

7

Time Synchronization over Ethernet

- Network Time Protocol (NTP)

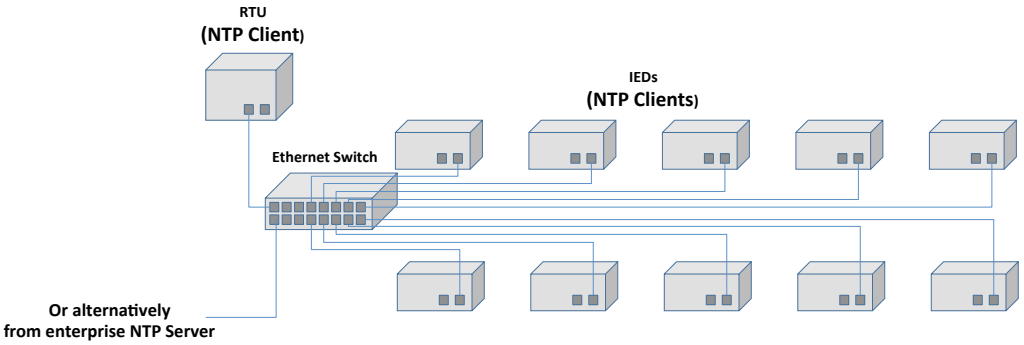


NovaTech

8

Time Synchronization over Ethernet

- Network Time Protocol (NTP)

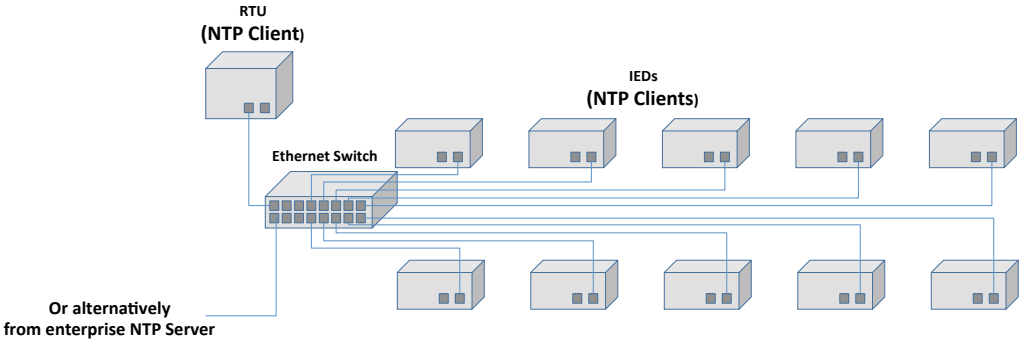


NovaTech

9

Time Synchronization over Ethernet

- Network Time Protocol (NTP)
- Sufficiently accurate for SER applications
- Not sufficiently accurate for phasor measurement ("PMU") applications

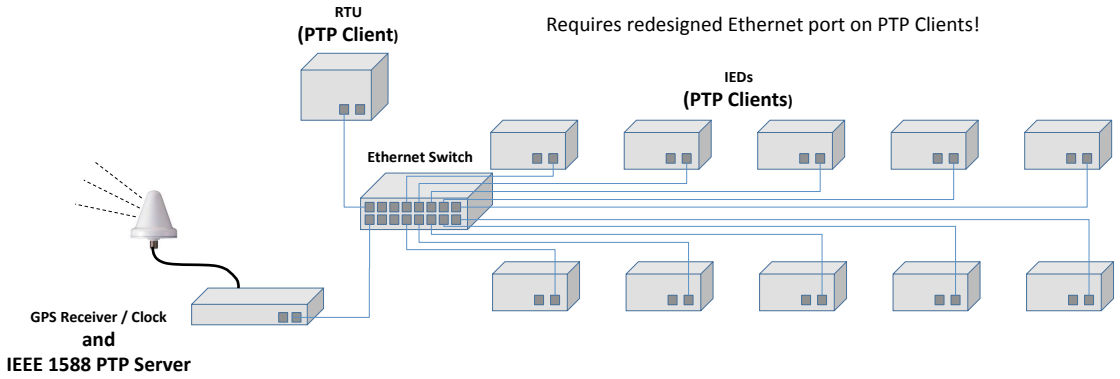


NovaTech

10

Time Synchronization over Ethernet

- IEEE 1588 Precision Time Protocol (PTP)
- Sufficiently accurate for phasor measurement ("PMU") applications

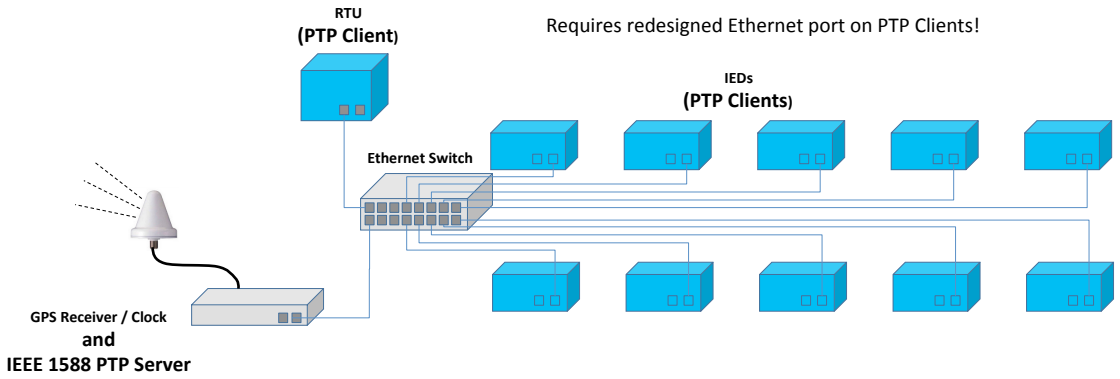


NovaTech

11

Time Synchronization over Ethernet

- IEEE 1588 Precision Time Protocol (PTP)
- Sufficiently accurate for phasor measurement ("PMU") applications



NovaTech

12

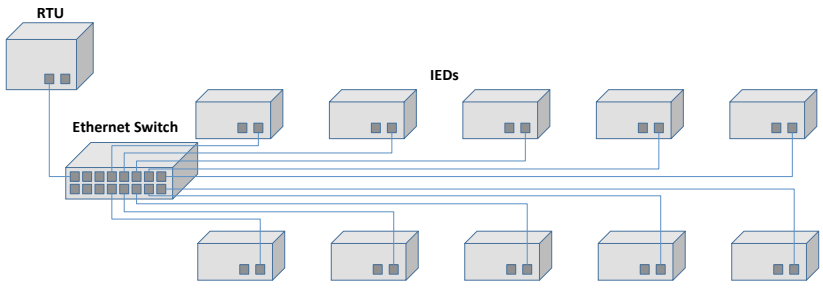
Expansion of Ethernet

- More Ethernet in Substations
- Time Synchronization over Ethernet
- IEDs with Built-in Switches

NovaTech

13

Conventional Networking Using Ethernet Switch

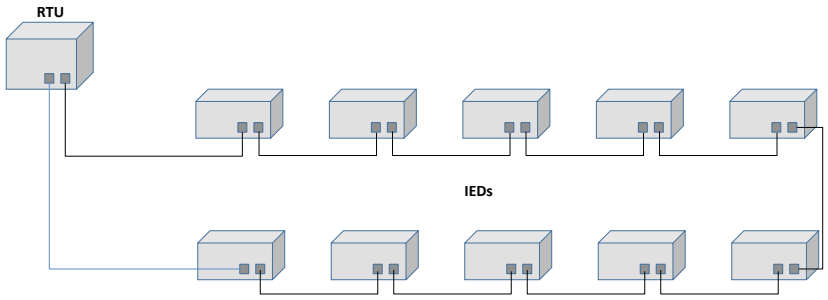


- **All connections are "point-to-point"**

NovaTech

14

IEDs with Built-in Switches

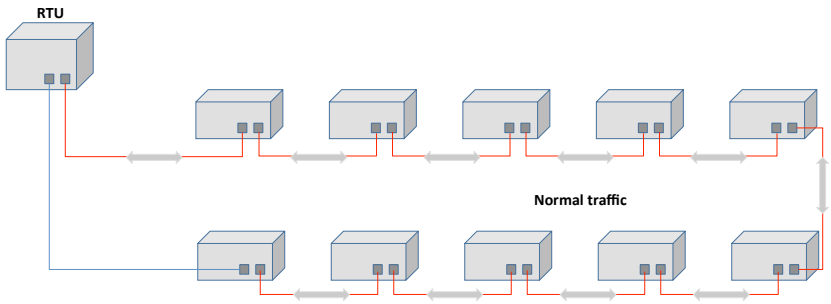


- Each IED has a switch built in
- Can form a ring
- Ring has higher availability

NovaTech

15

IED with Built-in Switches

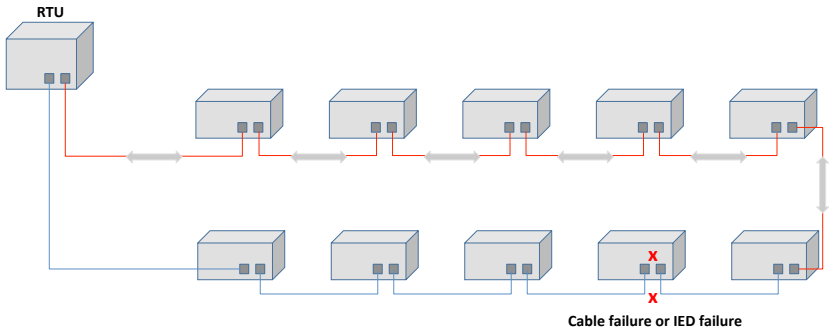


- Fault tolerance example

NovaTech

16

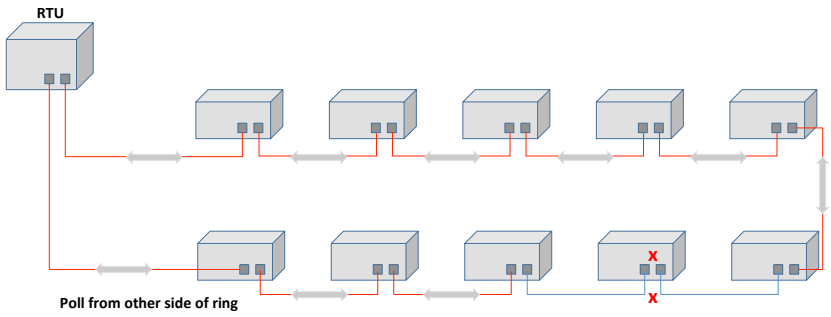
IED with Built-in Switches



NovaTech

17

IED with Built-in Switches



NovaTech

18

New Protocols

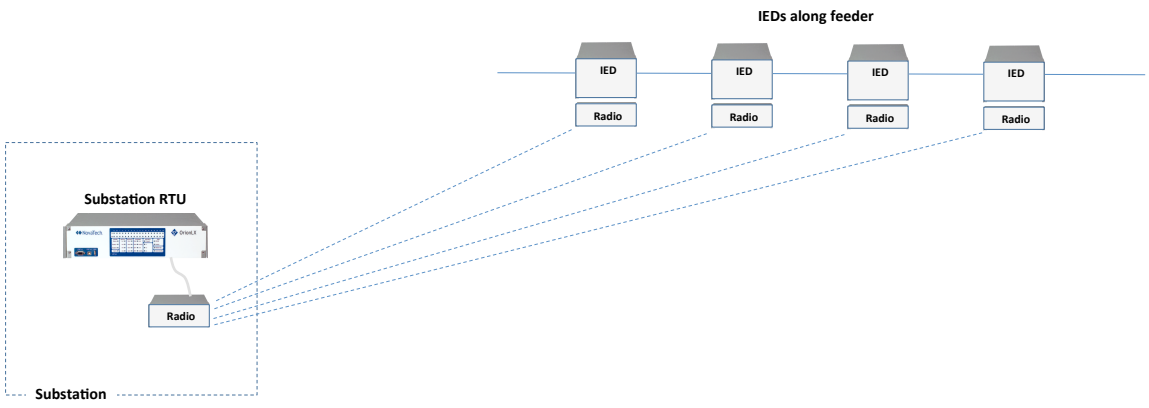
- DNP3 “Secure Authentication”
- IEC 61850

NovaTech

19

DNP3 with “Secure Authentication”

- Mid-Atlantic Application

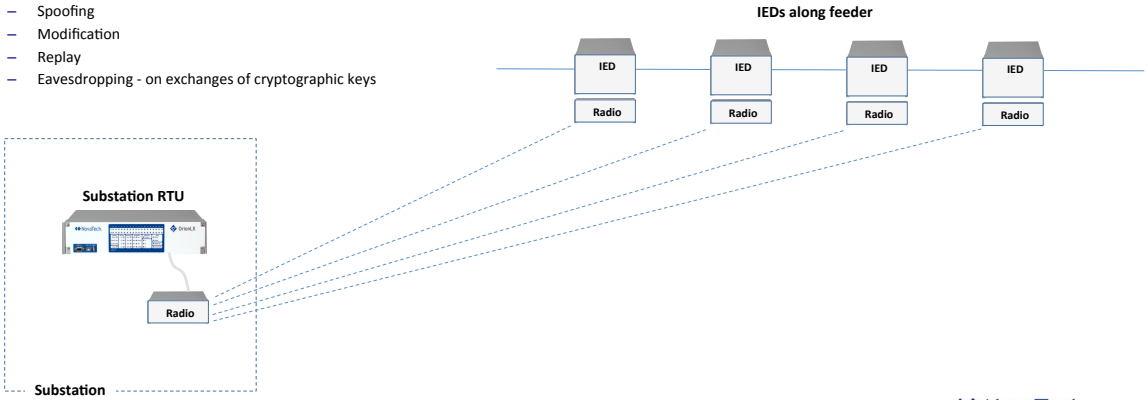


NovaTech

20

DNP3 with "Secure Authentication"

- The feeder-mounted IEDs can unambiguously determine they are communicating with the substation RTU
- The substation RTU can unambiguously determine it is communicating with feeder-mounted IEDs
- Vulnerabilities Addressed
  - Spoofing
  - Modification
  - Replay
  - Eavesdropping - on exchanges of cryptographic keys



NovaTech

21

Definitions

- Spoofing
  - A person or program successfully masquerading as another by falsifying data and thereby gaining an illegitimate advantage.
- Modification
  - Unauthorized changing of any portion of the data transferred between devices.
- Replay
  - Using a previously recorded or captured message to attack a computer system or network or to gain access to somewhere one is not authorized to be (a form of identity theft). Example: the sequence of DNP3 commands to get an RTU to trip a breaker might be recorded and replayed.
- Eavesdropping (on key transfer)
  - An unauthorized real-time interception of private communication, in this case the transfer of secret keys between DNP3 Master and Slave.

NovaTech

22

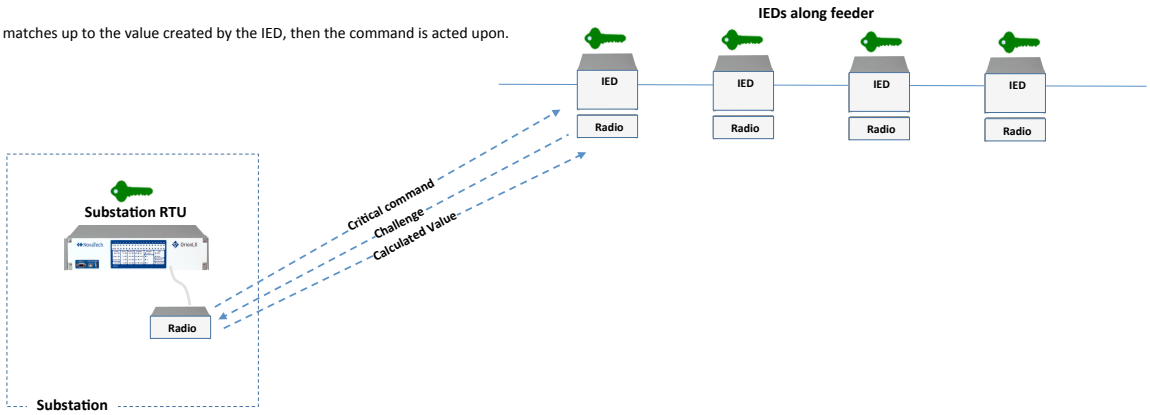
DNP3 Secure Authentication (Version 5) – How It Is Done

1) Both the Substation RTU and the feeder-mounted IEDs have secret keys

2) When the RTU sends a critical command to an IED (e.g a control command), the IED issues a challenge "Prove that you are who you say you are"

3) The RTU then has to send down a value calculated by the key

4) If this matches up to the value created by the IED, then the command is acted upon.



NovaTech

23

IEC 61850

- What problems are solved by IEC 61850
  - Establishes standardized names for all data in IEDs
  - IEDs all provide a standardized file that describes what data they contain and what they do ("pick lists")
  - The entire substation automation system can be designed at one time, using one tool.
  - Very high speed interlocking using "GOOSE" messages ("protection speed")
- More complicated and costly than DNP3
- Why so popular in the world market?
  - Fewer, larger utilities in places like Europe
  - International RTUs do not provide "pick lists" for IEDs. This makes 61850 appear novel.
  - Substation automation is mostly implemented by the "big four" international suppliers (ABB, Siemens, Alstom and Schneider).
    - Their costs are reduced when designing substation automations with all of their automation only.
    - They can manage the complexity.
- Why not so popular in the US?
  - Most substation automation is implemented by users; the complexity and cost scares users off.
  - US RTU suppliers provide "pick lists" which simplifies configuration. 61850 does not appears as novel.
  - Most substation automation in the US is already implemented at low cost compared to European designs

NovaTech

24

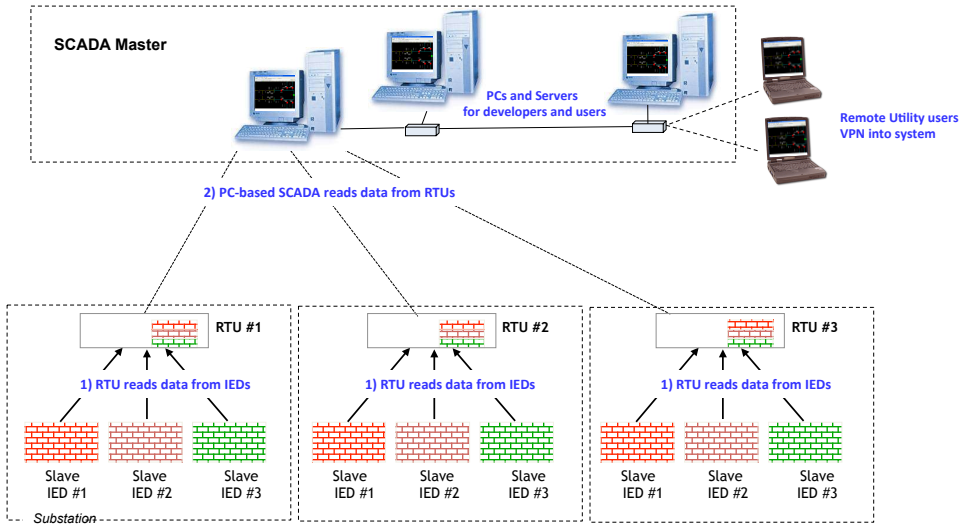
Web-Based SCADA and Traditional PC-Based SCADA
Main Difference

- PCs and Servers contain all the software in traditional PC-Based SCADA
- The Automation Processors ("RTUs") contain all the software in Web-based SCADA
  - PCs only browse

NovaTech

25

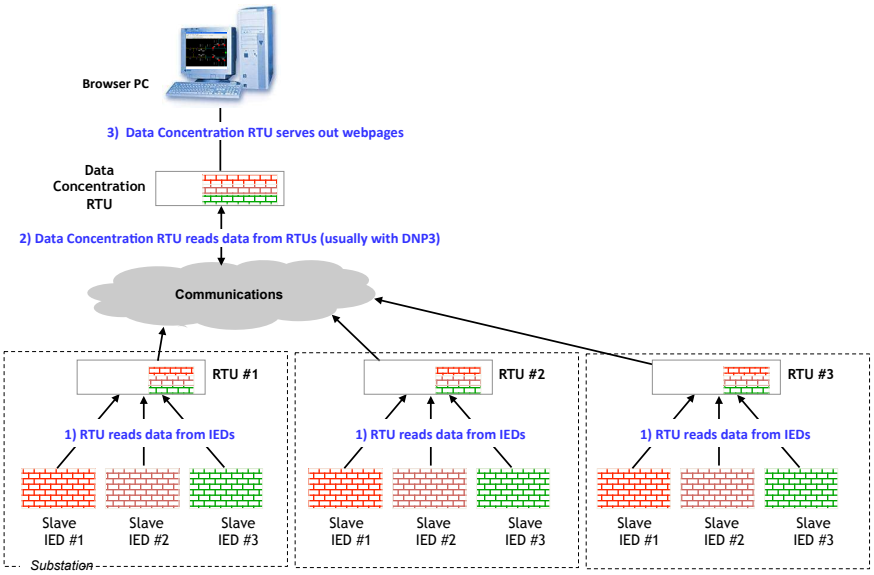
Traditional PC-based SCADA



NovaTech

26

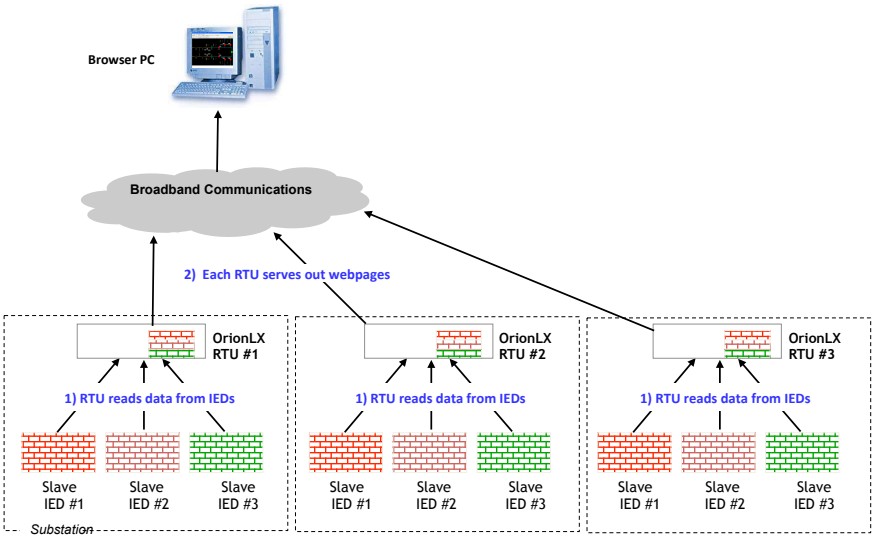
Web-Based SCADA



NovaTech

27

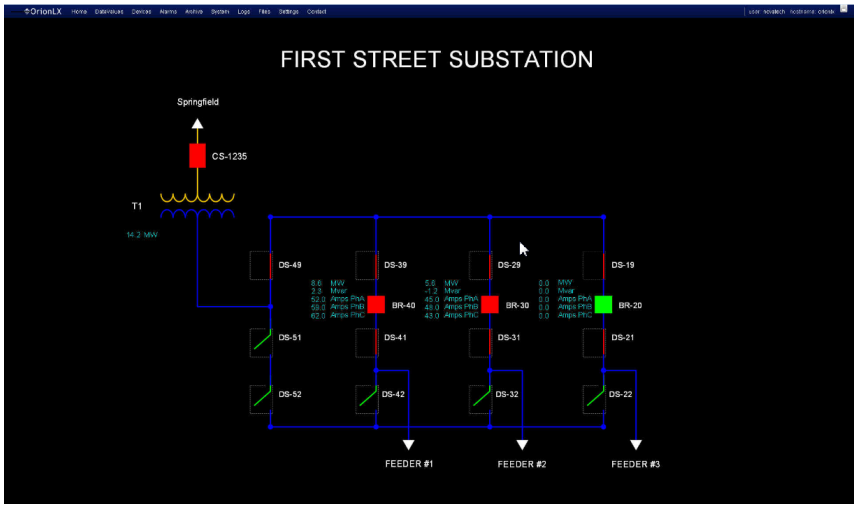
Distributed WEBserver SCADA



NovaTech

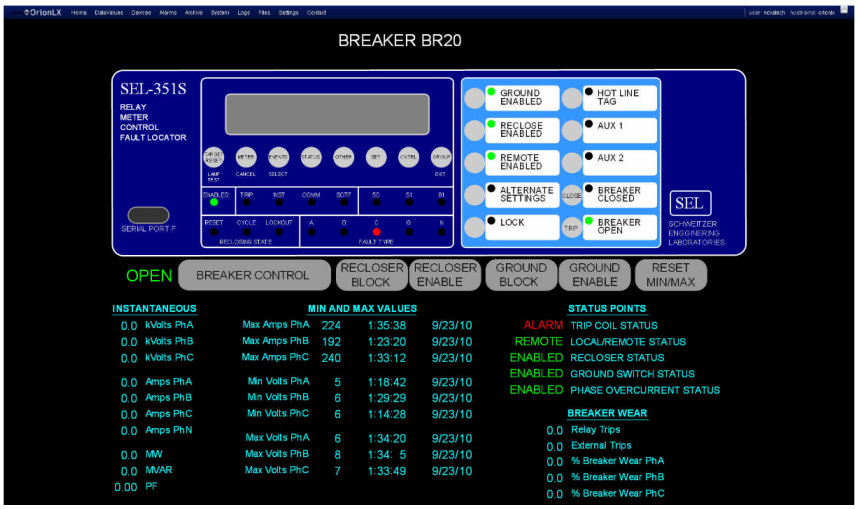
28

One-Line Diagram



NovaTech

Typical Breaker Zoom Screen



NovaTech

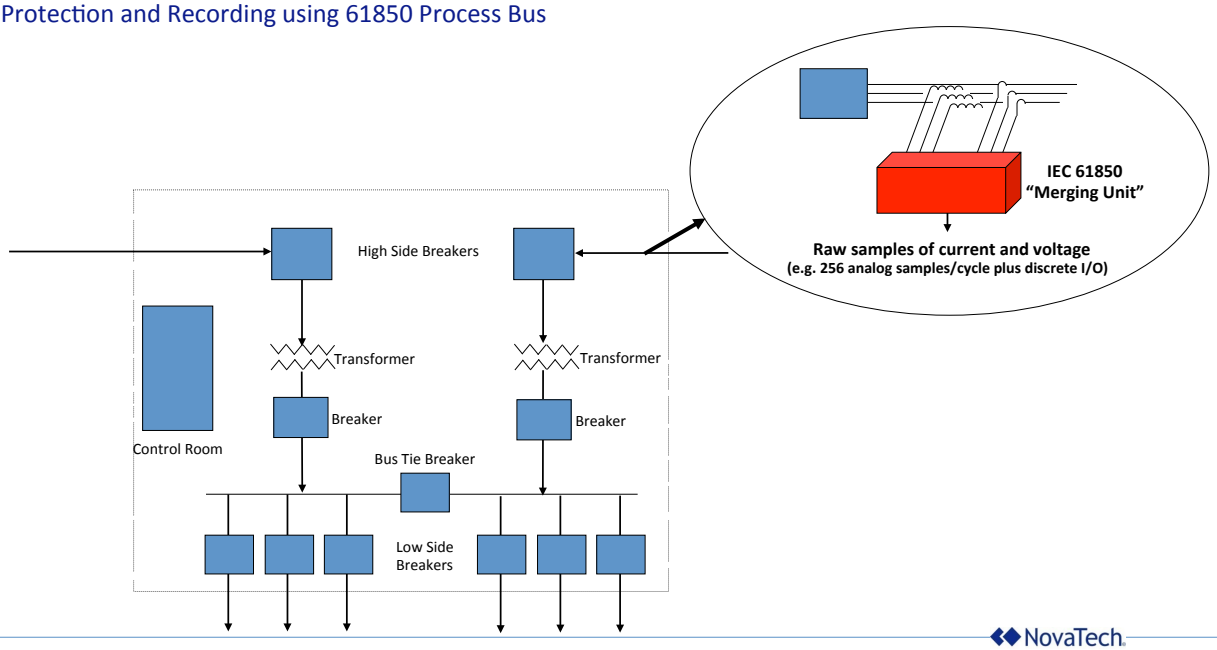
Substation Automation Strategies for the Future

- Box Consolidation
- Getting Data from IEDs Instead of from Hard-Wired I/O
- Expansion of Ethernet
  - More Ethernet Inside Substations
  - IEDs with Built-in Switches
  - Time Synchronization over Ethernet
- New Protocols
  - DNP3 "Secure Authentication"
  - IEC 61850
- Web-Based SCADA Instead of PC-Based SCADA
- Protection using 61850 Process Bus
  - Distributed Measurement, centralized protection

NovaTech

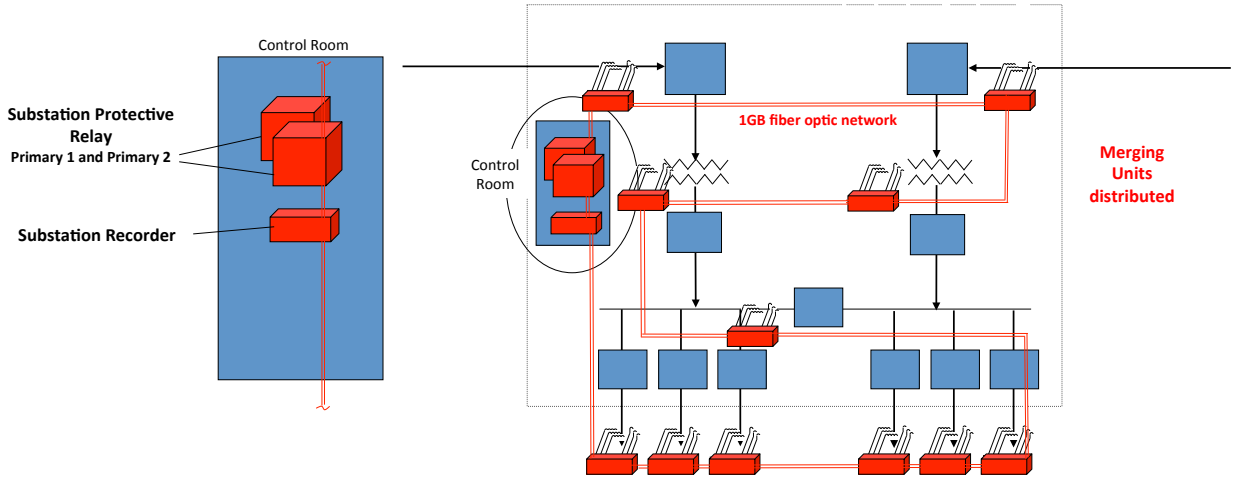
31

Protection and Recording using 61850 Process Bus



NovaTech

Protection and Recording using 61850 Process Bus



NovaTech

33

Thank You

NovaTech

34