Substation & Distribution Automation, Protocols and Security Issues

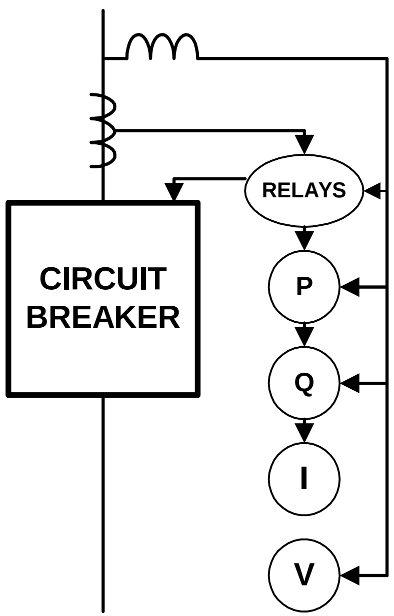
William J. Ackerman

Principal Consultant

WE'VE MOVED SINCE LAST SUMMER

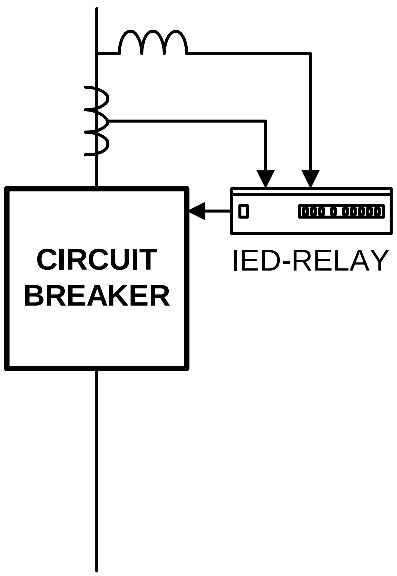
SA, DA, Protocols, DR and Security

Substation Data - The Old Way



- DATA AND CONTROL
- 3 - SINGLE PHASE CURRENTS
- 1 - THREE PHASE WATTS
- 1 - THREE PHASE VARS
- 3 - BUS VOLTAGE (1 SET PER BUS)
- 1 - TRIP/CLOSE STATUS & CONTROL
- 1 - RECLOSER STATUS & CONTROL
-

Substation Data - The New Way



DATA AND CONTROL QUANTITIES

REAL TIME VALUES

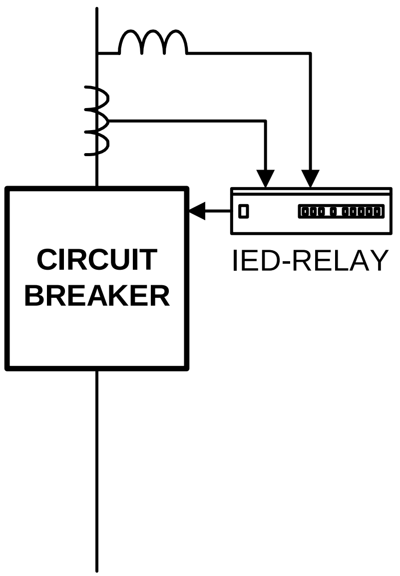
I_a, I_b, I_c, I_n, I_+, I_-, I_0	Mag. and Angle	14 points
V_a, V_b, V_c, V_+, V_-	Mag. and Angle	10 points
KW_a, KW_b, KW_c, KW_3		4 points
$KVar_a$, $KVar_b$, $KVar_c$, $KVar_3$		4 points
KWH_a, KWH_b, KWH_c, KWH_3		4 points
$KVarH_a$, $KVarH_b$, $KVarH_c$, $KVarH_3$		4 points
Frequency, Power Factor		2 points
Distance to Fault		1 point

DEMAND VALUES

I_a, I_b, I_c, I_n	(Magnitude and angle)	8 points
KW_a, KW_b, KW_c, KW_3		4 points
$KVar_a$, $KVar_b$, $KVar_c$, $KVar_3$		4 points

SA, DA, Protocols, DR and Security

Substation Data - The New Way



DATA AND CONTROL TO EMS

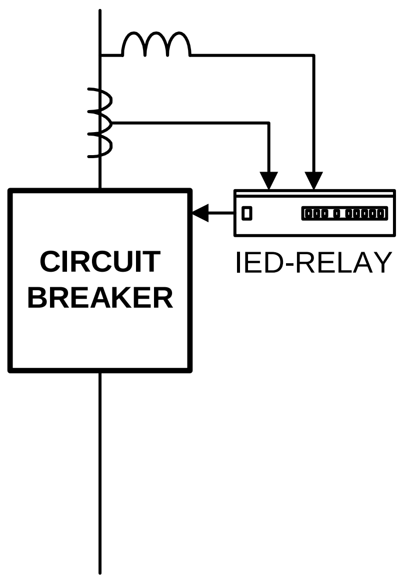
STATUS POINTS (Minimum of 27)

Breaker	Recloser	Ground Protection
O/C Protection 1	O/C Protection 2	O/C Protection 3
Base Settings	Alt 1 Settings	Alt 2 Settings
Zone Sequence	Spring Charging	Single-shot Reclose
Multi-Shot Reclose	Open Command	Close Command
Event Capture 1	Event Capture 2	Waveform Capture
Neg. Seq. Time O/C	Pos. Seq. Dir O/C	Neg. Seq. Dir O/C
Trip Coil Monitor	Clear Recl Counters	Breaker Fail Initiate
Sync Check On/Off	Sync Check Bypass	Local/Supv

CONTROL POINTS (Minimum of 18)

Trip	Close	Recloser Enable
Recloser Disable	Enable O/C Prot 1	Enable O/C Prot 2
Enable O/C Prot 3	Enable Base Settings	Enable Alt 1 Setting
Enable Alt 2 Setting	Enable 1-shot Recl	Enable Multi-Recl
Enable Event Capt 1	Enable Event Capt 2	Enable Wave Capt
Enable Sync Check	Bypass Sync Check	Local/Supv

Substation Data - The New Way



DATA AND CONTROL

SUMMARY	
Real Time Values	43
Demand Values	16
Maximum Values	36
Minimum Values	36
Status Values	27
Control Points	18
OTHER DATA:	
Fault Records	32
Operations Records	128
Load Profile Records	3,840
Waveform Samples	14,336
Power Quality Data	4,000

Substation Data - Old and New

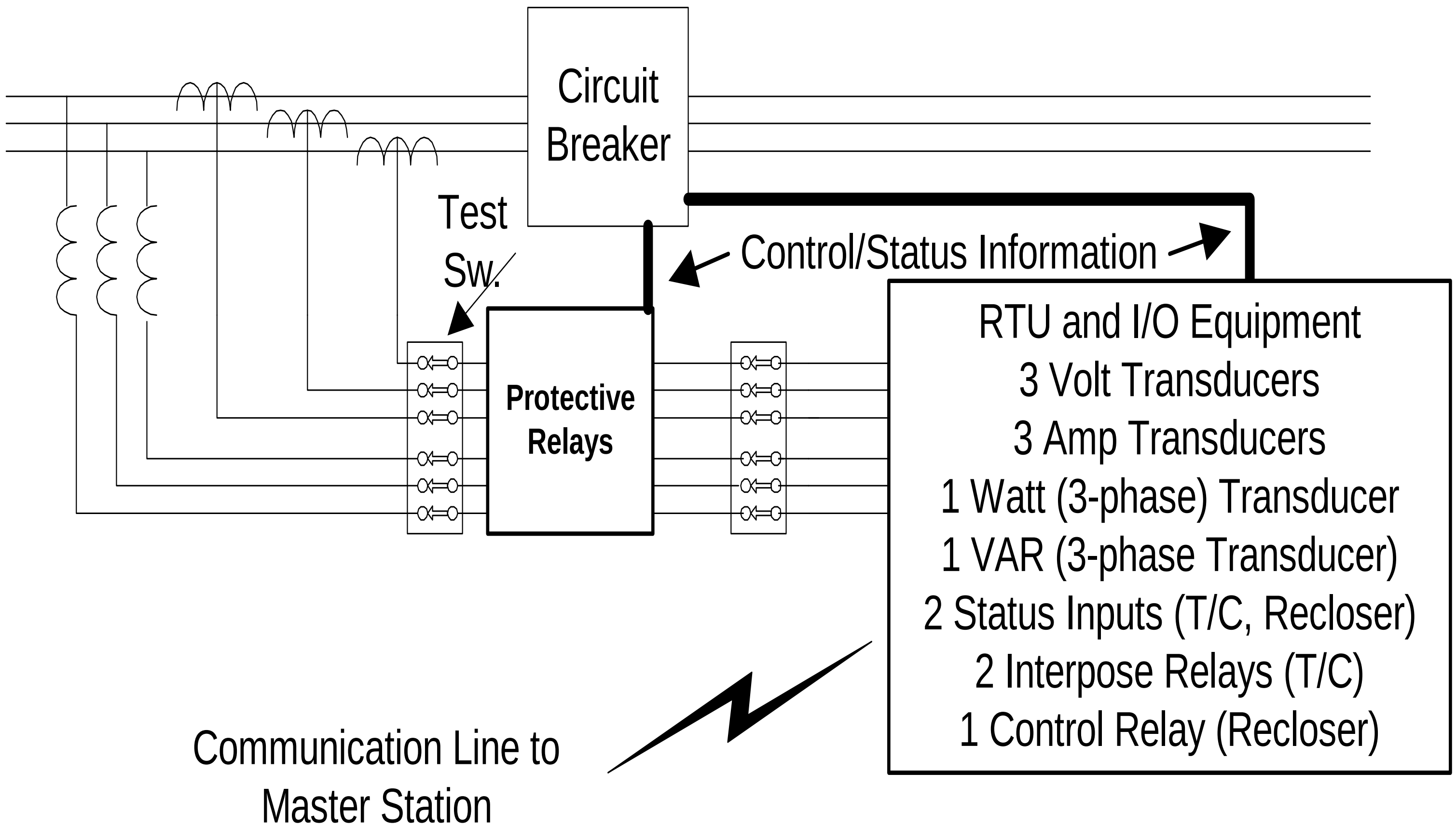
10 FEEDER SUBSTATION, REAL TIME VALUES ONLY

(2 Incoming Lines, 2 Transformers)

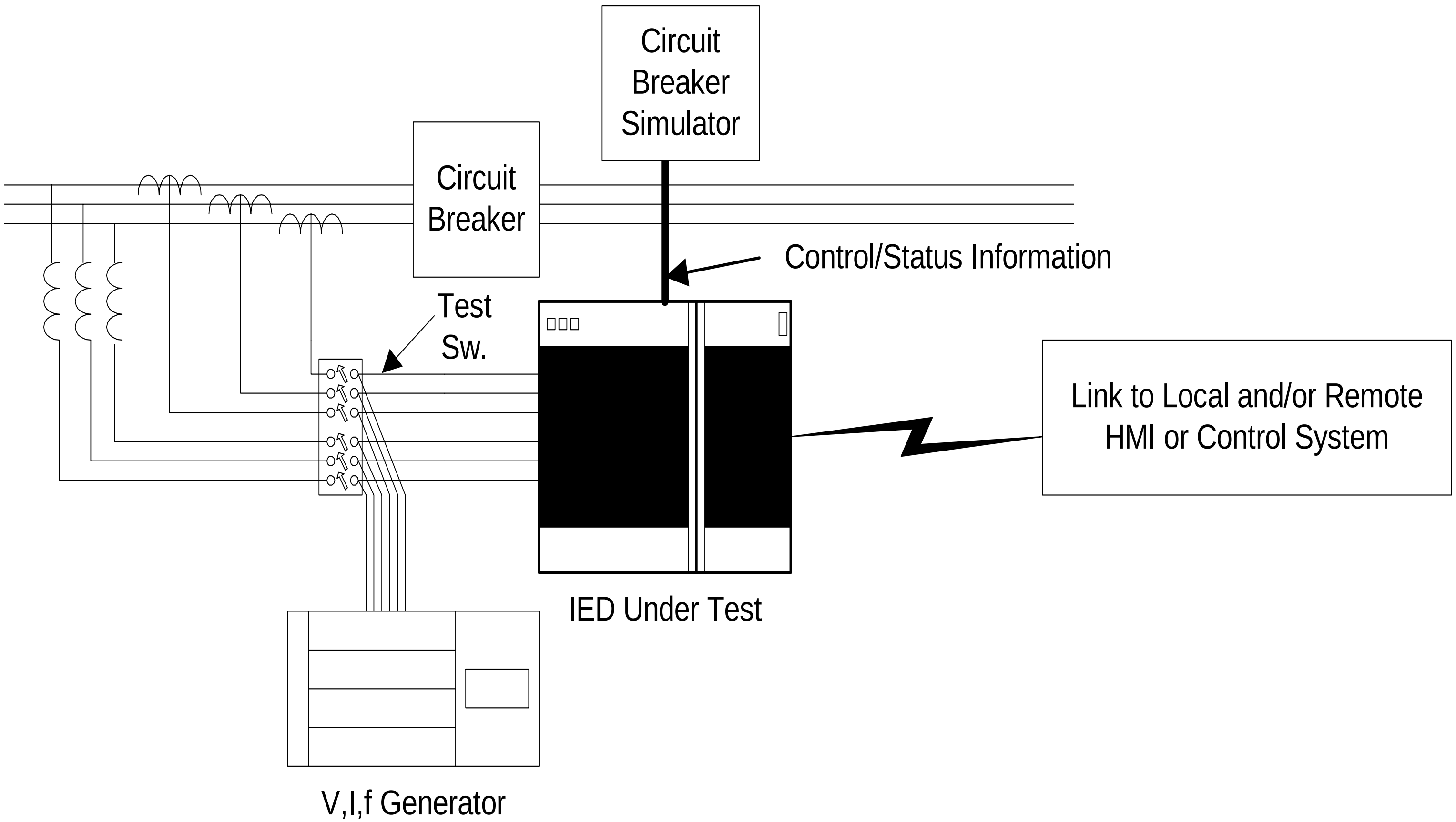
	RTU BASIS	IED BASIS
ANALOGS	82	602
STATUS	24	378
CONTROL	24	252
	130	1232

REAL-TIME DATABASE CAN BE ALMOST TEN TIMES LARGER WHEN IEDs ARE USED!

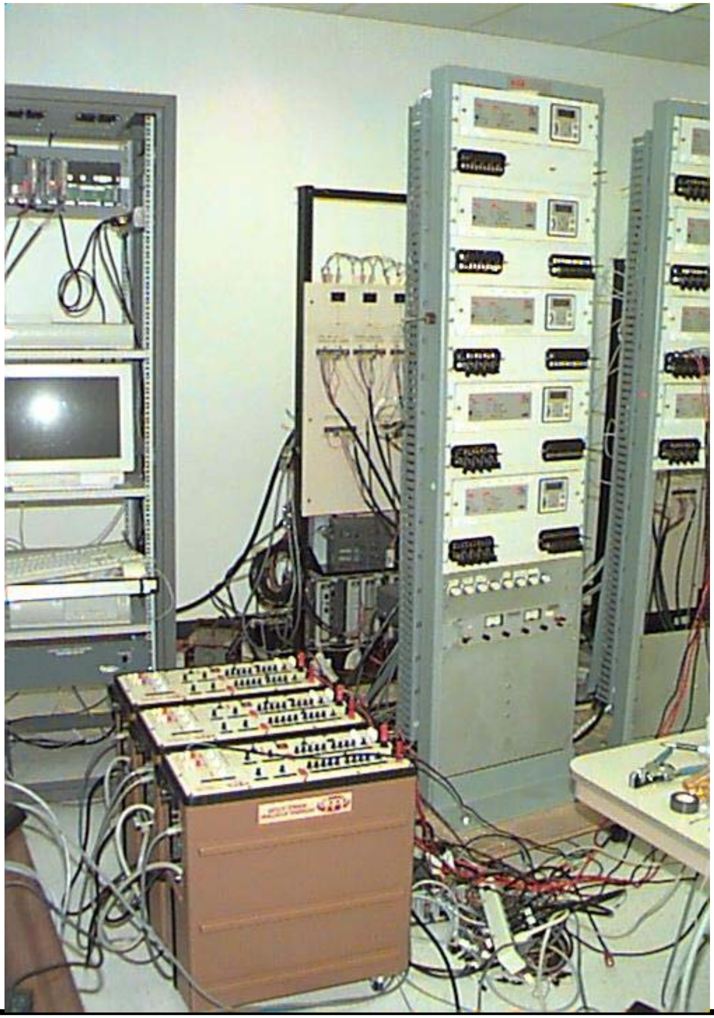
SA, DA, Protocols, DR and Security



SA, DA, Protocols, DR and Security



SA, DA, Protocols, DR and Security



Substation Data - Old and New

10 FEEDER SUBSTATION, REAL TIME VALUES ONLY

(2 Incoming Lines, 2 Transformers)

	RTU BASIS		IED BASIS	
	Points	Checks	Points	Checks
ANALOGS	82	574	602	4214
STATUS	24	48	378	756
CONTROL	24	48	252	504
	130	870	1232	5474

Status Checks: on/off (2)

Control Checks: on/off (2)

Analog Checks: -max, -norm, -act, 0, +act, +norm, +max (7)

SA, DA, Protocols, DR and Security

- Consider "simple" PLC automation scheme with 5 possible outputs determined by 15 inputs (3 single-phase voltages from 5 devices, low,normal,high value)
  - Need to test ~$1.2\text{x}10^6$ possible input combinations!
  - 6 tests per hour using generators = ~70 years
  - This appears to be somewhat unreasonable
  - Redesign such that outputs are dependent upon phase-B voltage from 5 devices
  - Now only need to test 3,000 possible combinations!
  - 6 tests per hour using generators = 63 days
  - Still somewhat unreasonable
  - FINAL SOLUTION: DO SOME SPOT CHECKS AND PRAY!

SA, DA, Protocols, DR and Security

- **NEAR-TERM IMPACT OF DATA VOLUME**
  - **New methods for building database essential**
    - **Use substation and/or device templates for replication**
    - **Pre-define standard objects**
      - **(Careful, there is no such thing as two identical substations)**
    - **Use object symbols, drag and drop to database**
    - **New naming conventions may be required**
      - **(Just when you got everybody to understand and use the old ones)**
    - **Greater use of default values on limits, etc.**
      - **(Careful, once a default, always a default)**

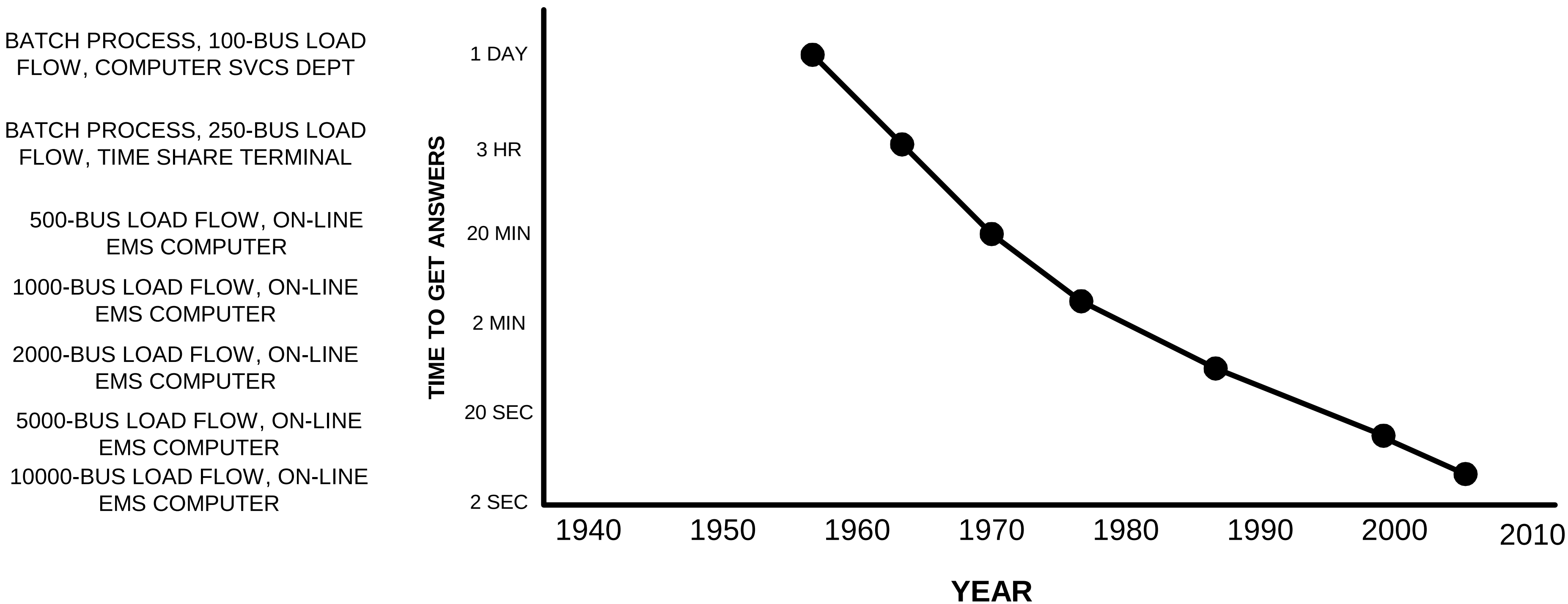
SA, DA, Protocols, DR and Security

- **NEAR-TERM IMPACT OF DATA VOLUME**
  - **New methods for maintaining database essential**
    - **Each new IED means hundreds of points**
    - **Need some technique to insure that nothing else changed when adding/deleting items**
    - **Saving field changes for a monthly database update probably won't work**
    - **Current checkout techniques will take too long to be practical**

SA, DA, Protocols, DR and Security

- **NEAR-TERM IMPACT OF DATA VOLUME**
  - **Performance Issues**
    - **10 to 100 times greater CPU power?**
    - **10 to 100 times additional disk storage?**
      - **Disk access times?**
      - **Shadow disks?**
    - **Can 2-second status and 10 second analog scans be maintained?**
      - **Upgrade communications facilities to higher bit rates to handle more data per unit time**
      - **Re-define a lot of status and analog points as slower scan or demand only**

A LITTLE PERSPECTIVE



SA, DA, Protocols, DR and Security

- **NEAR-TERM IMPACT OF DATA VOLUME**
  - **Database Integrity and Failover Issues**
    - **Report and process by exception essential**
    - **Revisit deadbands and how they are defined**
      - **Make deadband definition more complex than a simple percent**
    - **What is impact of deadband on subsequent calculations?**
      - **(Greater deadband equals less useful results?)**

SA, DA, Protocols, DR and Security

- **NEAR-TERM IMPACT OF DATA VOLUME**
  - **Database Integrity and Failover Issues (continued)**
    - **Need to reconsider periodic check-point of complete database**
      - **Check-point by exception?**
    - **Not enough time to do periodic integrity scan of entire RT database**
      - **Break integrity scan into smaller groups, checked less often**
    - **Complete initializing scan after failover may take too long**
      - **Scan times much greater than actual CPU failover times**

SA, DA, Protocols, DR and Security

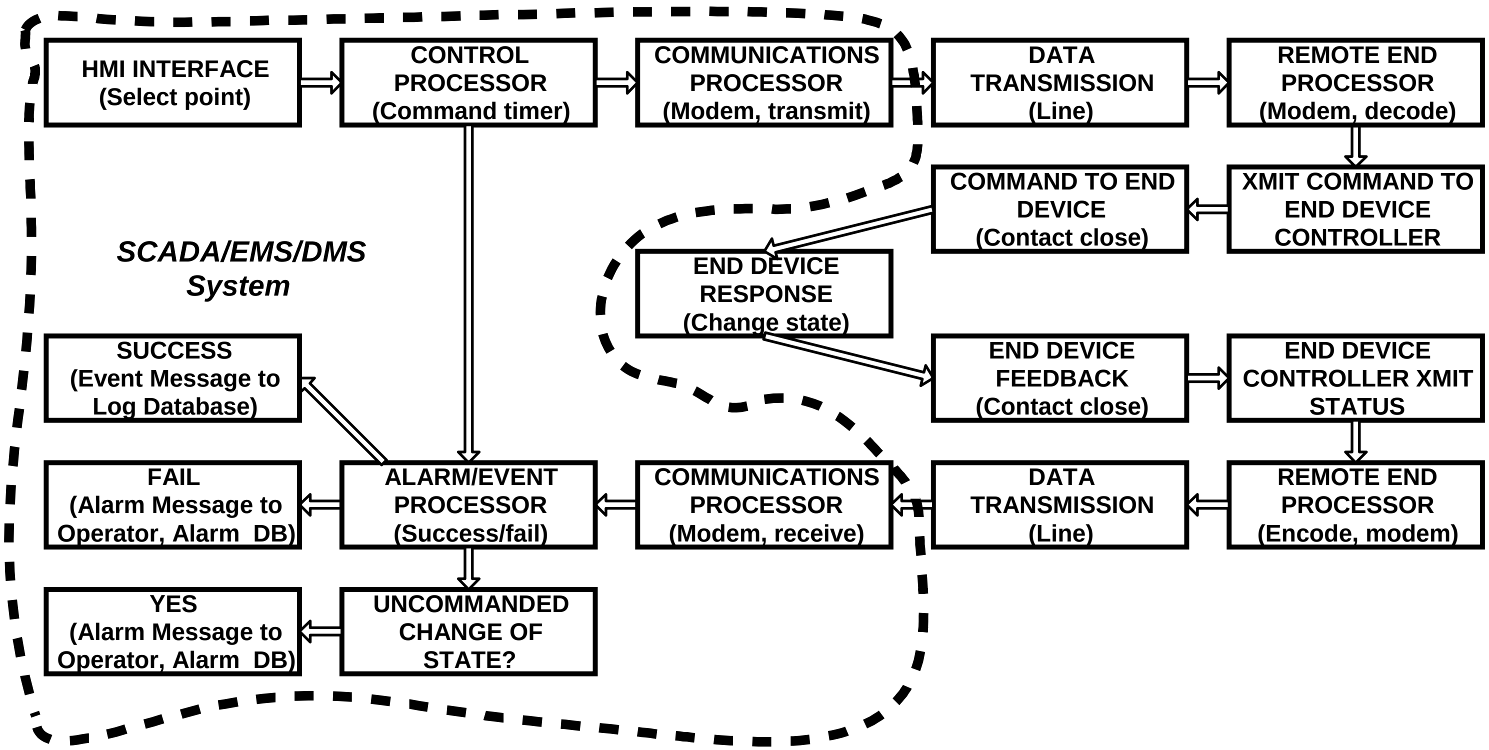
- **NEAR-TERM IMPACT OF DATA VOLUME**
  - **Alarm and Event Processing**
    - **Alarm priority structure will require complete re-design**
      - **Alarm processing can't be deterministic any more**
        - **A single IED can generate many alarms from one power system event**
        - **Multiple IEDs in the same or nearby substations may see the same event**
      - **Human factors design critical**
        - **Can't swamp dispatcher/operator during disturbance conditions**
        - **Dispatcher/operator needs to see every alarm during quiet conditions**
    - **Significant disturbance = 200,000 alarm burst?**
    - **Alarm and event record retention criteria needs review**
    - **Alarm and event search tools must be more user friendly**

SA, DA, Protocols, DR and Security

- **NEAR-TERM IMPACT OF DATA VOLUME**
  - **Supervisory Control Issues**
    - **Control sequences no longer deterministic (fixed times)**
    - **Control response a function of the IED involved**
      - **(Some are fast, some are slow)**
    - **Dispatcher/Operator no longer has “feel” about control completion time**
      - **(Need supplemental information per point on control speed?)**
    - **“Check before Operate” may not be**

SA, DA, Protocols, DR and Security

Importance of Real-Time



SA, DA, Protocols, DR and Security

- **LITIGATION DATABASE**
  - In the near future a “Litigation” Database may be as important as an Operations Database.
  - All events adverse to open access (i.e., tripping of relays causing interruptions or denial of transfer capability, inability to deliver per contract, etc.) will require full documentation and justification that the events were truly technically necessary.
  - Full documentation of such events must be easily accessible as quickly as possible after the event so that appropriate responses can be prepared.

SA, DA, Protocols, DR and Security

PROTOCOL ISSUES – HISTORY --- Mid 1980's

- **Substation Device Interfaces**
  - **Urgent Need for a standard Substation IED Protocol**
  - **Many competing vendor, utility "standards"**
- **IEEE-PES Substations Committee**
  - **Responded with Interim Solution**
    - **IEEE Standard 1379: "Trial Use Recommended Practice for Data Communications between Intelligent Electronic Devices and Remote Terminal Units in a Substation"**
      - **DNP 3.0, Level-2**
      - **IEC 60870-5-101, 2, 3, 4, 5**
      - **"Trial Use" designation provides limited lifetime**
      - **(DNP3.0 initially was designed as an implementation of an IEC 60870 protocol)**

SA, DA, Protocols, DR and Security

- **PROTOCOL ISSUES - HISTORY**
  - **IEEE-1379 Updated in 1999, “Trial Use” designation removed**
  - **IEEE-1379 specifies two recommended protocols**
    - **DNP 3.0**
    - **IEC 60870-5-101, 2, 3, 4,5**
  - **Many other protocols being used today**
    - **Modbus, Modbus+ (Very popular)**
    - **ASCII (Slow, but comprehensive)**
    - **Incom, CONITEL, SC1801, CDC Type 2, etc. (Obsolete)**
  - **Future Protocol Direction**
    - **UCA Compatible**

SA, DA, Protocols, DR and Security

PROTOCOL ISSUES

UCA (Utility Communications Architecture)

- Version 1 issued December 1991
  - Part of EPRI Project RP2949, Integration of Utility Communication Systems
  - Mostly Functional Descriptions
  - Not widely adopted by industry because of lack of details
  - Manufacturing Messaging Specification (MMS)(ISO/IEC 9506) to be used for real-time data but specific implementations missing

SA, DA, Protocols, DR and Security

- **UCA (Utility Communications Architecture) is NOT a protocol**
- **UCA is a set of rules and techniques for achieving enterprise-wide common communications procedures**
- **There are many protocols that may be UCA-compliant**
- **The utility industry is seeking to achieve a common, universal, *<u>inter-operable</u>* protocol for all SUBSTATION data interchange (including control) that is UCA-compliant**
- **Ultimately, *<u>inter-changeability</u>* is desired (but will probably never occur)**

SA, DA, Protocols, DR and Security

- **UCA is NOT "Plug and Play"**
- **Communications in a Substation Use "Publish and Subscribe" Technology**
- **Addition of a new device (a relay, for example)**
  - **Install, wire, assign unique address(es)**
  - **Program new device to listen for, and respond to, messages from other specific devices**
  - **Program all other applicable devices to listen for and respond to messages from new device**

SA, DA, Protocols, DR and Security

PROTOCOL ISSUES

UCA/MMS Forum started in May 1992

Six working groups to consider MMS applications

1. Power Plants
2. Control Centers
3. Customer Interfaces
4. Substation Automation
5. Distribution Feeder Automation
6. Profiles

WGs 1, 2, 3 not very active

WG 4, 5, 6 functions have been absorbed into UCA-2.0™ Users Group

SA, DA, Protocols, DR and Security

PROTOCOL ISSUES

- Inter-Utility Control Center Real Time Data Exchange
  - Power system data
  - Interchange Scheduling data
- Initial Protocols based on Regional Needs
  - WSCC (Western Systems Coordinating Council)
  - IDEC (Inter-Utility Data Exchange Committee)
  - ELCOM (European)
- Above Groups, Vendors, Users Wanted one Standard
  - Name adopted was ICCP
    - Inter Control Center Communications Protocol

SA, DA, Protocols, DR and Security

PROTOCOL ISSUES

- Utility Communications Specification Working Group Established
  - EPRI RP-3830-01
  - Work started September 1991, soon merged with IEC efforts
  - Result issued as IEC International Standard
    - Common U.S. name is ICCP
    - Common International name is TASE.2
      - Telecontrol Application Service Element 2
      - IEC 60870-6-503, -505, -702, and -802
  - TASE.2 utilizes MMS, is UCA compatible
  - Over 200 Utilities using ICCP in U.S.
  - NERC Mandate to use ICCP for Data Exchange

SA, DA, Protocols, DR and Security

Protocol Issues

UCA In the Substation

- UCA Version 2 Specification issued Late 1996
- EPRI transferred rights on UCA-2.0™ documentation to IEEE
- IEEE Published UCA-2.0™ documents as a technical report (TR-1550) which is available to the public
- UCA-2.0™ Users Group and IEC TC-57, WG 10,11,12 coordinate efforts to produce a common protocol document

SA, DA, Protocols, DR and Security

PROTOCOL ISSUES

- UCA-2.0™ Meetings and Demonstrations held in conjunction with IEEE-PES Power Systems Relay and Substations Committees (3 times per year)
- Vendors demonstrate latest product achievements and interoperability

SA, DA, Protocols, DR and Security

PROTOCOL ISSUES

- **Substation Automation**
  - **GOMSFE**
    - **(Generic Object Models for Substation and Feeder Field Devices)**
    - **Non-vendor specific**
    - **Compliance with Power System Object Model descriptions**
    - **IEDs became available mid-1998 for interoperability demonstrations, but didn't support all features (and many still don't)**
    - **Currently at Version 0.9x**
  - **GOOSE**
    - **(Generic Object Oriented Substation Event)**
  - **GSSE**
    - **(Generic SubStation Event)**

SA, DA, Protocols, DR and Security

- **Agreement on a common language is ‘UCA compliant’ but not necessarily inter-operable:**
- **English French**
- **Spanish Swedish**
- **Arabic Chinese**
- **etc.**

SA, DA, Protocols, DR and Security

- **Agree on 'English' as common language -- still not 100% interoperable**

• **<u>U.S. English</u>**	**<u>British English</u>**
• **Windshield**	**Windscreen**
• **Hood**	**Bonnet**
• **Tire**	**Tyre**

SA, DA, Protocols, DR and Security

- **Agreement on “U.S. English” does not guarantee interoperability:**

- **<u>“Northern” English</u>** **<u>“Southern” English</u>**
- **Hello** **Hey**
- **Everybody** **Y’all**

SA, DA, Protocols, DR and Security

- **Agreement on “Northern” English does not guarantee interoperability:**

• **<u>Brooklyn</u>**	**<u>Boston</u>**
• **Toity**	**Thirty**
• **Harvard**	**Havad**

SA, DA, Protocols, DR and Security

- Inter-operability requires every data message to be self-contained, and not dependent upon any outside information. Result is a lot of overhead---very inefficient communications, but at 10 Mb/S or 100 Mb/S, this usually isn’t a problem (However, at 9600 b/S it’s impractical)

SA, DA, Protocols, DR and Security

UCA is not "efficient"

Time in milliseconds to get one status value:

Min # of Bits	1200	160	32
Bit Rate	**UCA**	**DNP3.0**	**CONITEL**
1200 b/s	1000	133	27
2400 b/s	500	67	13
9600 b/s	125	17	*3*
1 Mb/s	1.2	0.16	*0.032*
10 Mb/s	0.12	0.016	*0.0032*
100 Mb/s	0.012	0.0016	*0.00032*

SA, DA, Protocols, DR and Security

- **Why Standardize Models**
  - Vendor independent
  - Simplify definition of device data
  - Maximize reuse of data component definitions
  - Reduce development and maintenance costs
  - Allow expanded market of suppliers
  - Allow flexibility in product design

SA, DA, Protocols, DR and Security

- **Object Model Requirements**
  - Topology and protocol independent
  - Standard representation of IED Data (definition and data type) for communication interoperability
  - Extensible (levels of standardization)
  - Allow vendors to differentiate products with value-added specialized functions

SA, DA, Protocols, DR and Security

- **“Settled” issues:**
- **Fiber optics will be physical media in HV substations, copper may be ok in LV**
- **Ethernet will be transmission technique**
  - **Ethernet speed is not specified; 10 Mbit, 100 Mbit, 1 Gbit available (but different speeds not inter-operable)**
- **MMS will be communications services**

SA, DA, Protocols, DR and Security

Some other observations:

1. **Ethernet is a definition of how to format, address and transmit datagrams over some media; and how to handle any problems such as data collisions. It says nothing about what the data is.**

SA, DA, Protocols, DR and Security

2. MMS stands for Manufacturing Messaging Specification. It is an IEC Standard. It specifies how to perform services such as “send data”, “receive data”, “request data”, “no response”, “acknowledge”, etc. It says nothing about what the data is.

SA, DA, Protocols, DR and Security

3. **TCP/IP is actually two protocols:**

   Transmission Control Protocol

   Internet Protocol

SA, DA, Protocols, DR and Security

TCP is responsible for breaking up a message into datagrams, re-assembling them at the other end, re-sending anything that gets lost, and putting things back in the right order. It doesn't know anything about the message or its meaning.

TCP is connection-oriented---it confirms communications.

SA, DA, Protocols, DR and Security

4. UDP/IP is actually two protocols

User Datagram Protocol

Internet Protocol

SA, DA, Protocols, DR and Security

UDP provides port addressing and data-integrity layer on top of IP

UDP is Connectionless--- it does NOT provide any sequencing or datagram loss protection services. UDP must rely on repetition in hopes that at least one transmission get through.

SA, DA, Protocols, DR and Security

IP is responsible for routing individual datagrams

IPv4 is address-limited (32 bits), being replaced by IPv6 for more addresses (128 bits) , more features

TCP hands IP a datagram with a destination.

IP doesn't know how this datagram relates to any datagram before or after. It just gets it to the specified destination.

SA, DA, Protocols, DR and Security

- **IEEE P-1525 (PES Substations Committee) was to be U.S. standard that would result in interoperability of equipment. Failed in balloting and has been cancelled.**
- **IEC 61850 (TC57) is International standard that should result in interoperability of equipment**

SA, DA, Protocols, DR and Security

- A number of US personnel are balloting members of IEC, IEEE, UCA Committees
- UCA is in demo mode, No real published standards, will be incorporated into IEC-61850)
- IEC-61850 is in 10 parts, all are published as International Standards, Part 10, Testing, is last to be published
  - Part 1 is an excellent introduction and overview—available from the IEC offices in Switzerland
- No vendor has all UCA functions in a device

SA, DA, Protocols, DR and Security

Major Open Issues

- UCA communications ok for data, does not yet meet requirements for Protection
- Some tests and demos have generally not met speed requirements
- Many installations are still in “learning phase”
- Most Ethernet Equipment is not DC-operated
- Most Ethernet equipment has narrow operating temperature range (0^oC - 40^oC)
- RFI/EMC (IEEE C37.90) characteristics not tested in most Ethernet equipment

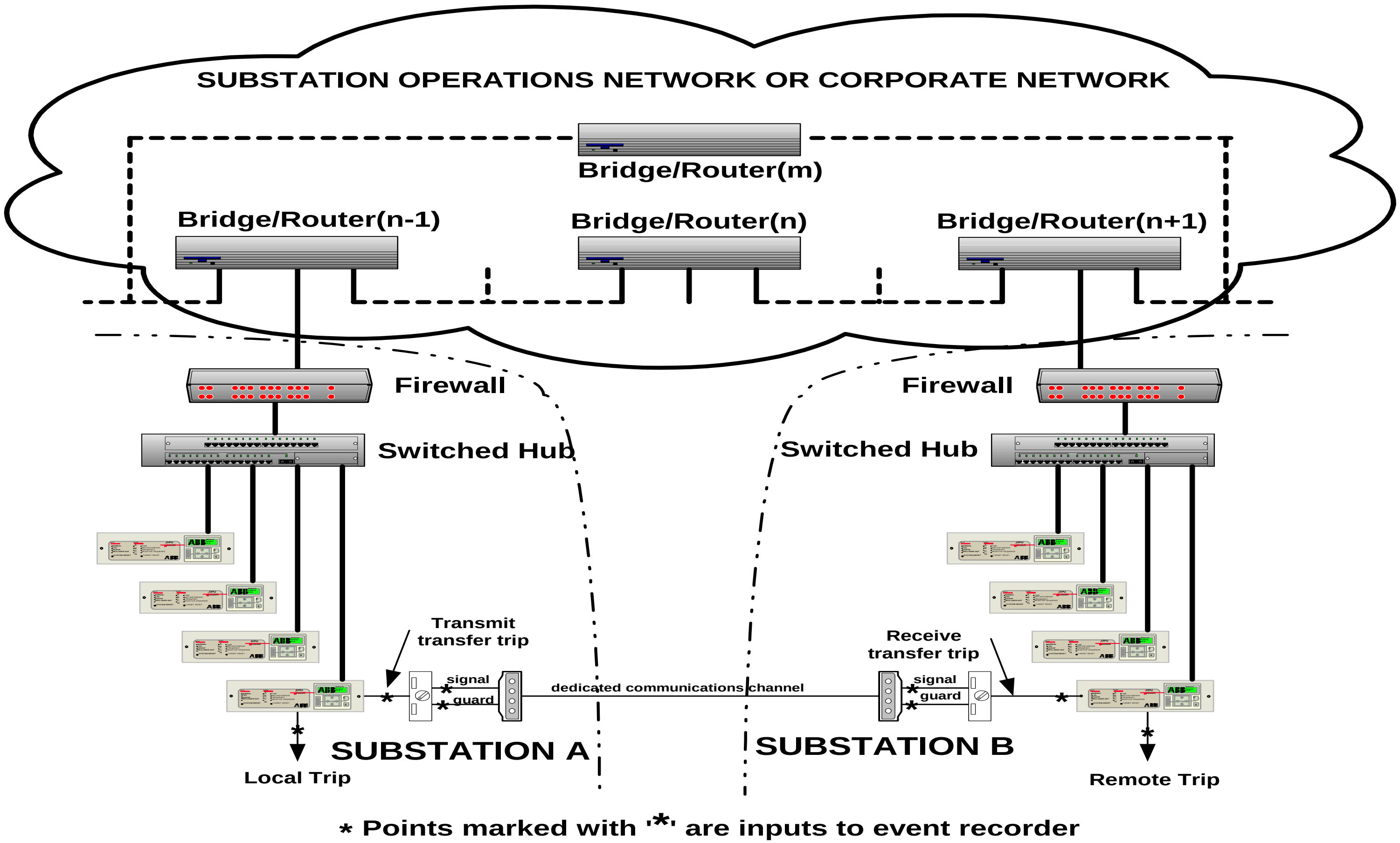
SA, DA, Protocols, DR and Security

UCA/Ethernet will use switched hub in substation to establish 'pseudo' determinism.

UCA Hub in substation will enable:

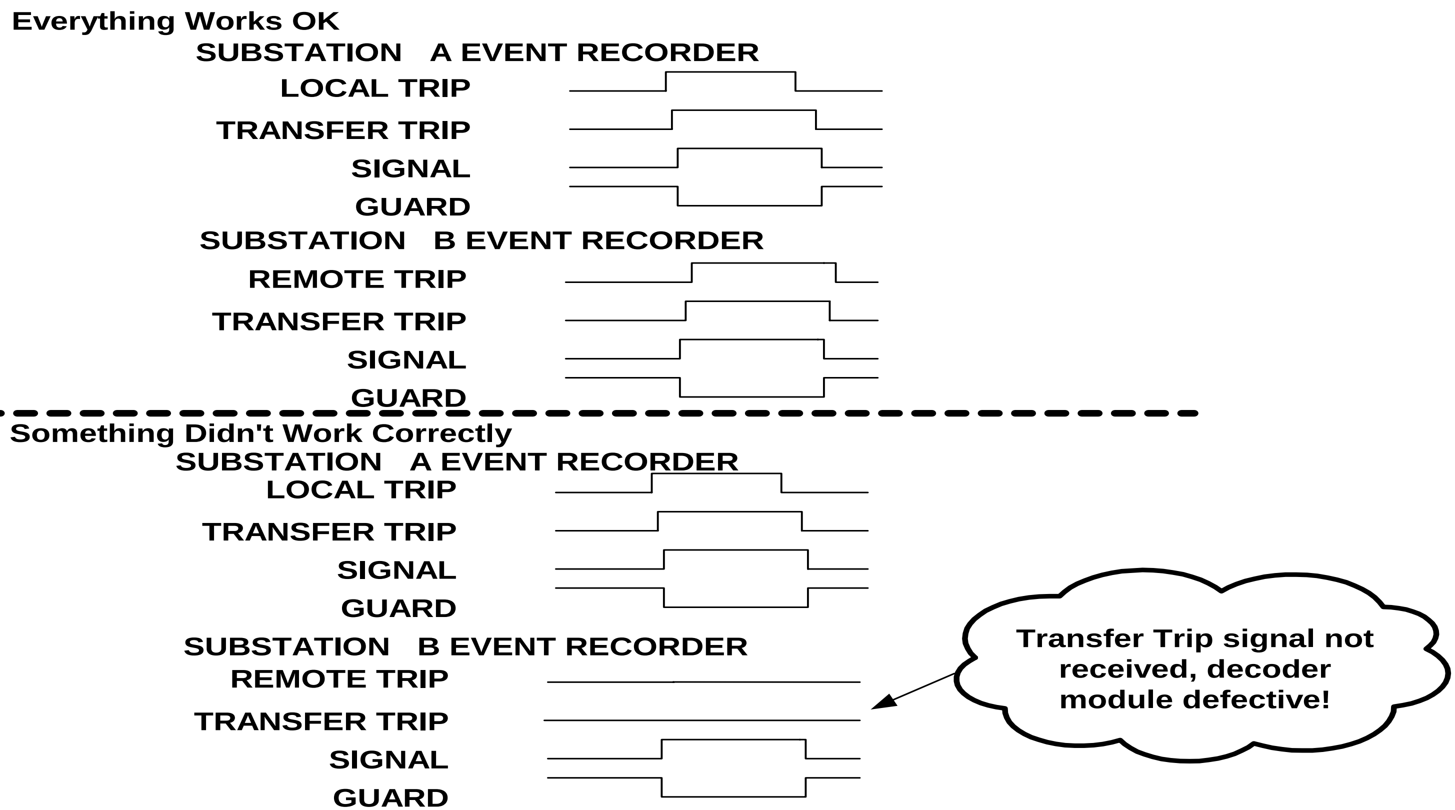
- Relay-to-relay communications
- Substation-to-substation communications
- Substation-to-desktop (via firewall) communications

SA, DA, Protocols, DR and Security

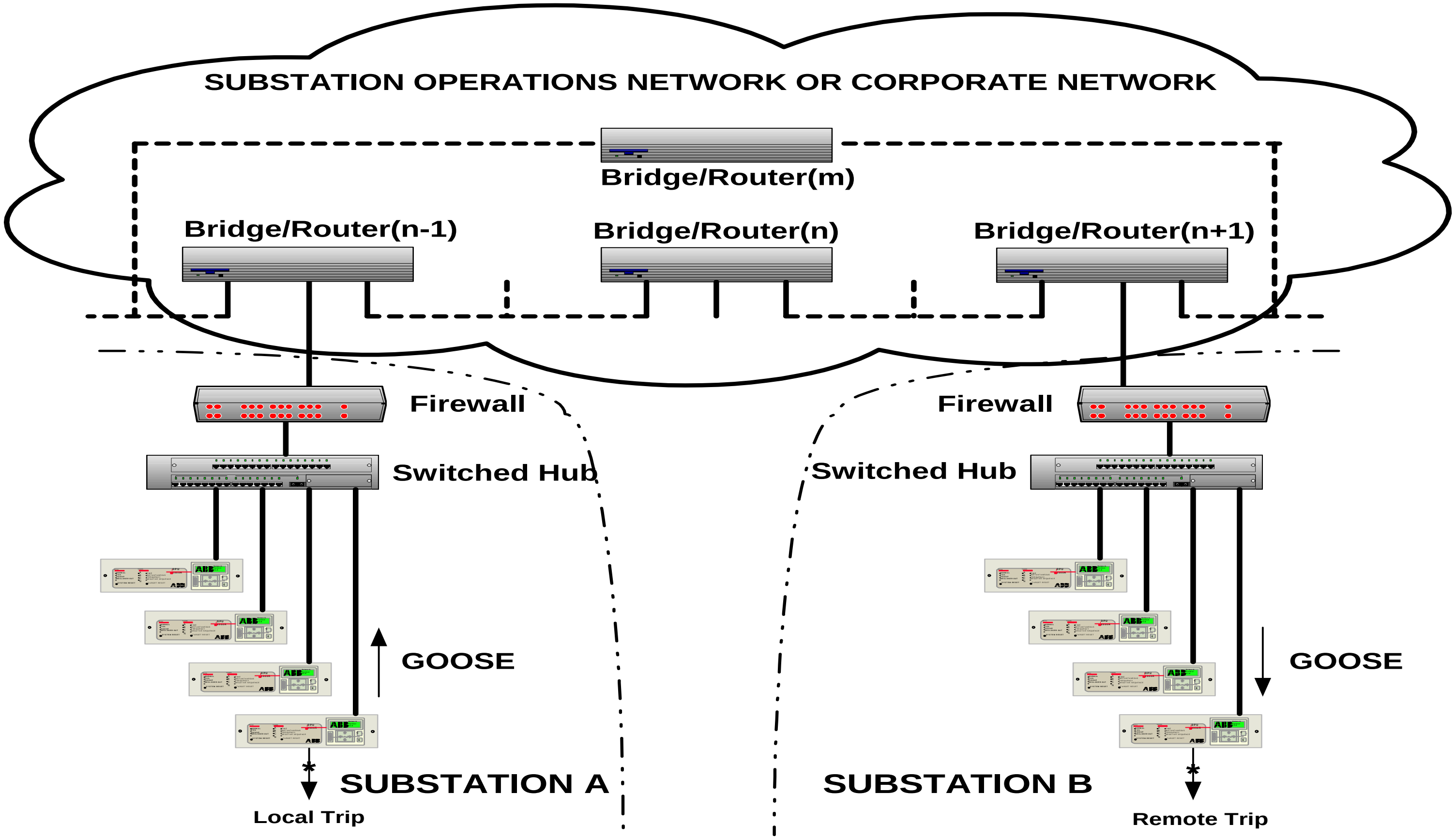


SA, DA, Protocols, DR and Security

EVENT RECORDER TRACES OF AN OPERATION ---
SUBSTATION TO SUBSTATION DIRECT CONNECTION



SA, DA, Protocols, DR and Security



SA, DA, Protocols, DR and Security

IEEE 1613

- Standard to define environmental characteristics of Ethernet equipment in substations
- Incorporates basic provisions of C37.90 series on SWC, EMI, RFI
- Applies only to substation equipment, NOT including protection
- Approved as IEEE Standard December 2002

SA, DA, Protocols, DR and Security

Major Open Issues

- Network maintenance tools for technicians still in infancy (Ethernet is not easy to troubleshoot)
- Security issues are just starting to be addressed
- UCA will require large amounts of software code in the end device
  - Unit Testing increasingly difficult
  - More opportunities for bugs

SA, DA, Protocols, DR and Security

Network Timing and Time Sync

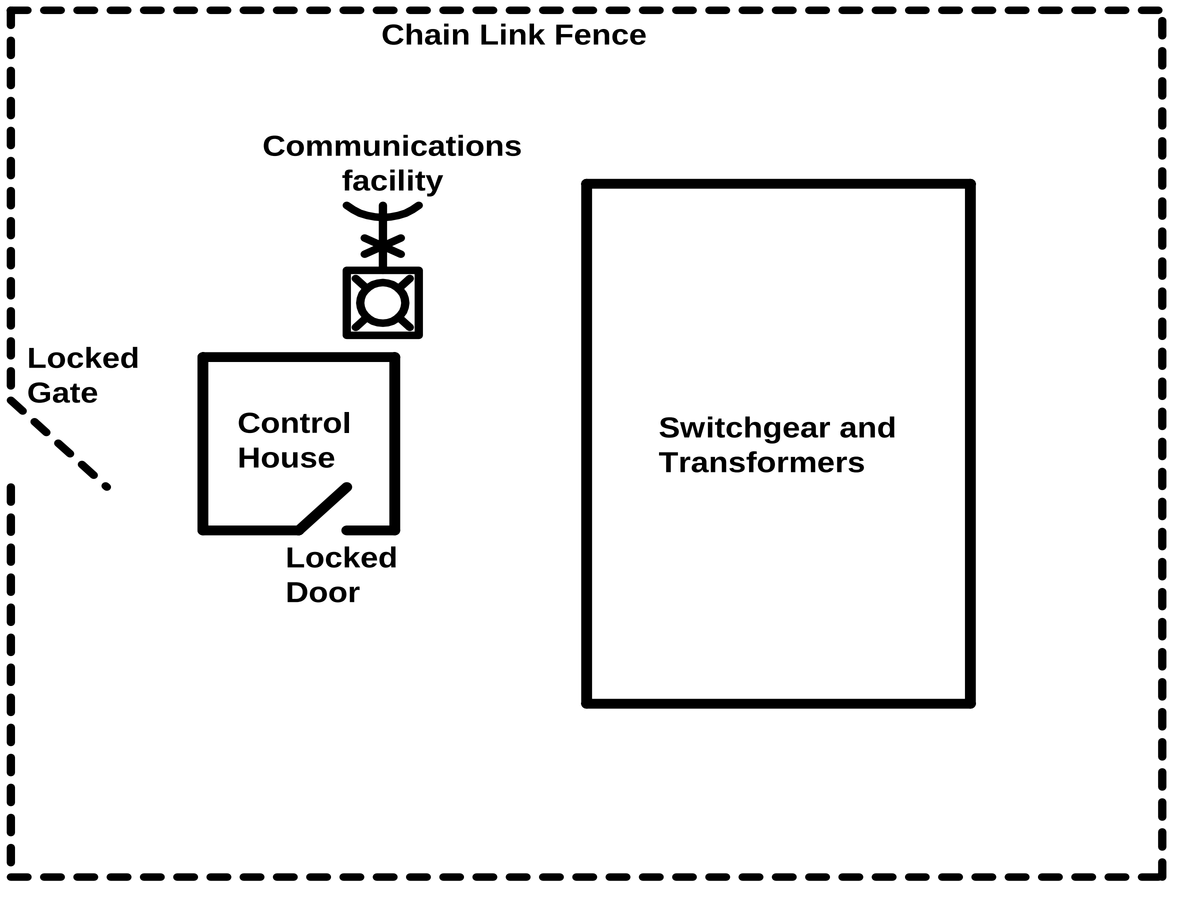
- Most common today is a GPS receiver with IRIG-B output, distribution to relays via a timing wire
  - Requires extra wiring, propagation delays in timing wire can impact accuracy
- IEEE Standard 1588 (approved July 2002) provides for ‘inexpensive’ time distribution over Ethernet and some other networks, with accuracy in the sub-microsecond range

SA, DA, Protocols, DR and Security

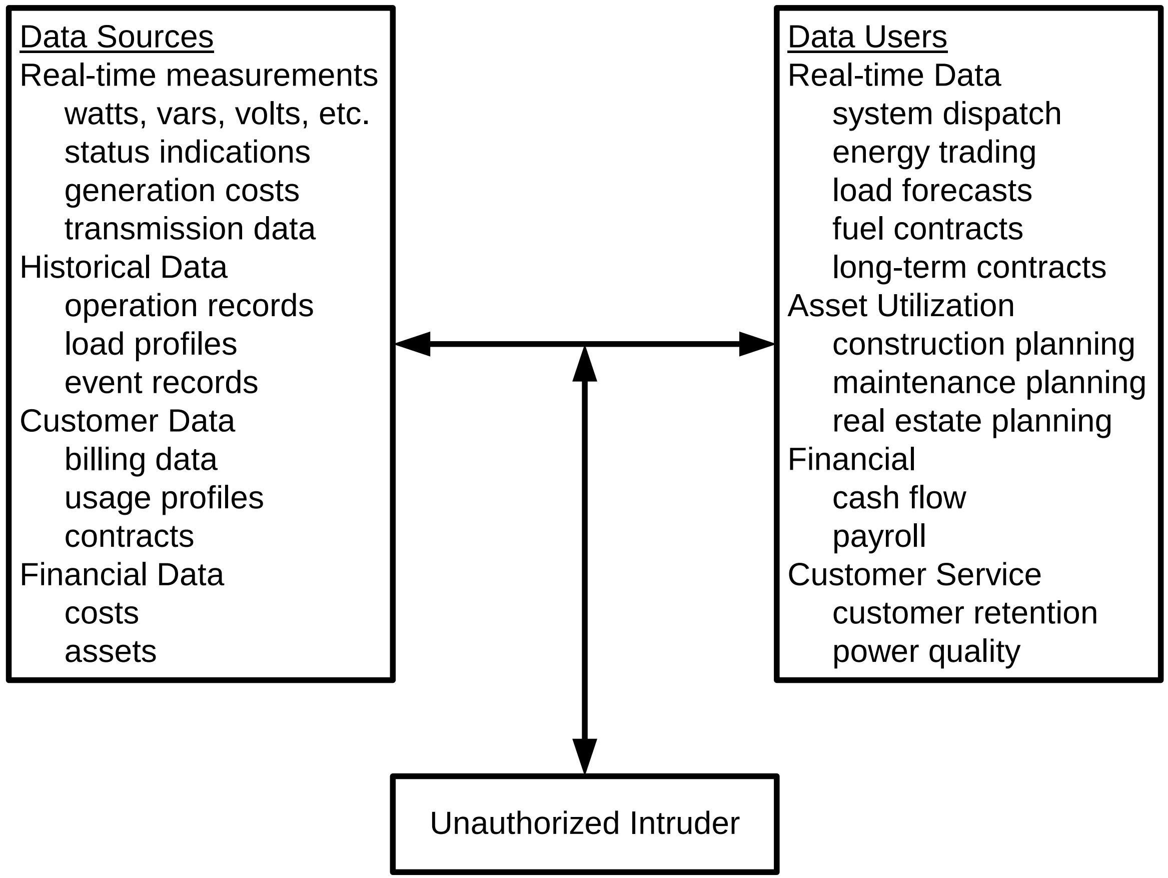
- **Is UCA-2.0™ the final 'One and Only' answer to protocol needs?**
  - Designed to meet practically all currently known requirements
  - Provides a defined 'single' protocol for the entire utility industry
  - Includes 'hooks' to add new functions in the future
  - Is rigidly structured, but very flexible

Security Issues

SA, DA, Protocols, DR and Security



SA, DA, Protocols, DR and Security



SA, DA, Protocols, DR and Security

Generation of Power

ACTION	IMPACT
Blocking transmission of data by introduction of random noise, corruption of data (‘denial of service’)	Impairment of economic dispatch, increased costs, mismatch between required and actual generation, cost to purchase replacement power for under-generation, excess generation without recovery of costs
Alteration of real-time production data	Impairment of economic dispatch, increased costs, mismatch between required and actual generation, cost to purchase replacement power for under-generation, excess generation without recovery of costs
Alteration of metering data	Bills rendered for less than actual amount delivered
Alteration of fuel cost information	Impairment of economic dispatch, increased costs, payment for fuel not used
Alteration of unit status data	Failure to operate at actual limits

SA, DA, Protocols, DR and Security

Transmission of Power

ACTION	IMPACT
Blocking transmission of data by introduction of random noise, corruption of data ('denial of service')	Fall-back to ultra-conservative operating practices on lines and transformers because of lack of knowledge of actual conditions
Alteration of real-time power flow data	Departure from optimum dispatch and system operation (at increased costs)
Falsified switching and tagging instructions to take lines, other equipment out of service	Inability to fulfill contracts, transfer limitations, non-economic operation of generation, inability to sell/buy power
Insertion of false status information regarding open/closed switches	Generation of false alarms in power system operation programs such as state estimator, topology, contingency analysis etc.

SA, DA, Protocols, DR and Security

Distribution of Power

ACTION	IMPACT
Blocking transmission of data by introduction of random noise, corruption of data (‘denial of service’)	Loss of visibility into distribution system, slow or no response to problems, potential safety problems
Altered transformer and line loading data	Operation of facilities above ratings, accelerated loss of life, bad data for load forecasting, violation of power quality and power delivery regulations
Altered status data	Undetected outages, violation of power quality and power delivery regulations
Altered switching and tagging information	Safety issues, including potential injury or death

SA, DA, Protocols, DR and Security

Power and Energy Trading

ACTION	IMPACT
Blocking transmission of data by introduction of random noise, corruption of data ('denial of service')	Inability to execute profitable transactions, cancel unprofitable transactions.
Altered quotation data	Significant cost penalties if transactions are entered at the wrong cost or selling price
Deletion or erasure of agreements	Loss or alteration of transaction records
Alteration of system conditions and status	Failure to enter into otherwise desirable or profitable transactions
Intercept confidential data regarding costs, system conditions	Use knowledge of costs and conditions to obtain competitive advantage

SA, DA, Protocols, DR and Security

Asset Management

ACTION	IMPACT
Blocking transmission of data by introduction of random noise, corruption of data (‘denial of service’)	Under-utilization because of need for conservative operations when actual conditions are unknown
Altered loading data	Overloading of assets with resulting loss of life, failure to perform proper preventive or corrective maintenance
Altered status data	Failure to protect apparatus, failure to perform preventive or corrective maintenance

SA, DA, Protocols, DR and Security

Customer Activities

ACTION	IMPACT
Blocking transmission of data by introduction of random noise, corruption of data ('denial of service')	Inability to detect power quality problems, including outages
Altered meter data	Under or over billing of customer

SA, DA, Protocols, DR and Security

Objectives of a Security Program

- Administration tools
  - Automatic
  - Human
- Confidentiality
  - Compartmentalization of information
- Integrity of Network and Data
- Availability of Network and Data
- Non-repudiation

SA, DA, Protocols, DR and Security

Sources of Threats

- Equipment failure
- Authorized user makes mistakes
- Authorized user exceeds authorization
- “Casual” intruder (curiosity)
- Intentional intruder
- Software bugs

SA, DA, Protocols, DR and Security

Recent advertisement by a network security vendor:

Your Network will *never, ever* be

100% Secure!

SA, DA, Protocols, DR and Security

What can be done:

- Limited Access
- Obscure, Non-standard Protocols
  - (Exact opposite of UCA objectives)
- Passwords, Other physical identifiers
- Firewalls
- One-way data transfer

SA, DA, Protocols, DR and Security

Conclusions:

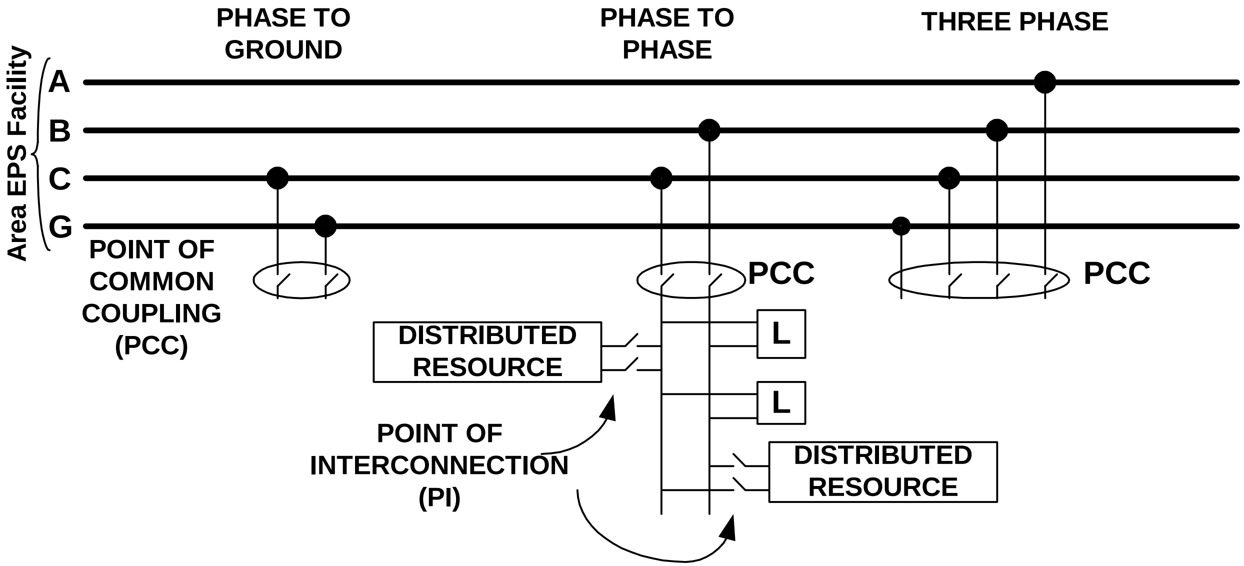
1. **The degree of effort expended by an intruder is directly related to the 'profitability' of the intrusion.**

2. **The degree of effort expended to protect against security breaches is directly related to the cost of a breach.**

Distributed Resources on the Distribution System

SA, DA, Protocols, DR and Security

- **Definitions:**



SA, DA, Protocols, DR and Security

- "User" Concerns
  - Safety of Personnel
    - Personnel must be able to work on the EPS and DER facility without undue risk of injury or death
    - General public should not be exposed to hazardous conditions
  - Fault duty, including DER, should not exceed ratings of distribution system equipment, including customer-owned equipment connected to the system
    - Equipment damage, downed conductors, vault fires, etc.
  - Normal load-carrying and interrupting capabilities, including DER, should not be exceeded
    - Reduction of system reliability, premature failure of equipment
  - Protective relaying and control equipment, should not be subject to mis-operation as a result of DER additions
    - More and longer interruptions, high/low voltage problems

SA, DA, Protocols, DR and Security

- **Producer and General Interest Concerns**
  - **Interconnection costs must be minimal**
    - **Interconnection equipment should be some fraction of the cost of the DER being connected.**
    - **Utility involvement should be minimized**
      - **Impact studies cost too much**
      - **Some utilities use interconnection standards as a means of ‘killing’ DER**
  - **Interconnection must be ‘simple’ so that it won’t discourage DER applications**
  - **Interconnection apparatus should be ‘maintenance free’ as much as possible**
  - **Interconnection operation should be ‘automatic’**

SA, DA, Protocols, DR and Security

- **Significant Problem Areas**
  - **Scaling**

    "My typical distribution feeder has a peak load of 4 Mw. Adding a few kW of PV is a whole different problem than adding 400 kW."
  - **Islanding**

    Utility is still responsible for voltage and frequency of all its customer connections. Creating an island where some utility customers are supplied with un-controlled voltage or frequency is unacceptable
  - **Safety**

    Personnel working on the distribution system MUST be protected from backfeed or accidental energization
  - **Protection System Design**

    Radial distribution line protection is designed and coordinated for 'one way' power flow. Bi-directional flow in some part or all of a feeder is a whole new world of problems
  - **Networked Distribution System**

    Consideration postponed to future updates

IN CONCLUSION:

SA, DA, Protocols, DR and Security

A “Plug” for the Substations Committee Annual Meeting:

Tampa, Florida

April 10-14

Meeting Website:

http://ewh.ieee.org/cmte/scam2005

SA, DA, Protocols, DR and Security

Subcommittee C0: Data Acquisition Processing and Control Systems

Treatment of all matters relating to data acquired within substations and control of substations

- Interfaces to Substation Apparatus
- Use of Transducers
- Protocols
- Computers used in Substations
- Sponsor and Promote New Technologies

SA, DA, Protocols, DR and Security

Working Group C1

Guidelines and Recommended Practices for the specification and use of computer-aided systems as applied to substation design, engineering, construction, maintenance and operation.

SA, DA, Protocols, DR and Security

Working Group C2

Application of New Technologies in Substation Monitoring and Control

Task Force C2TF1: Communications Networking Devices Installed in Substations

Task Force C2TF2

Use of Computer Technology in Substation Data Acquisition and Control

SA, DA, Protocols, DR and Security

Working Group C3

Electric Network Control Systems Standards

Review and Update of All Assigned ANSI/IEEE and IEEE Standards applicable to Substation Automation and Control

SA, DA, Protocols, DR and Security

Standards and Guides Assigned to C0

- IEEE-1379-2000: Recommended Practice for Data Communications between Remote Terminal Units and Intelligent Electronic Devices in a Substation

- IEEE 1613: Standard Environmental and Testing Requirements for Communications Networking Devices in Electric Power Substations

- P 1615: Recommended Practice for Network Communication in Electric Power Substations

SA, DA, Protocols, DR and Security

Standards and Guides Assigned to C0

- P 1646: Standard Communication Delivery Time Performance Requirements for Electric Power Substation Automation

- P C37.1: Standard for SCADA and Automation Systems

- C37.2: Standard Electrical Power System Device Function Numbers and Contact Designations

SA, DA, Protocols, DR and Security

SIGN UP ASAP FOR ANNUAL MEETING

http://ewh.ieee.org/cmte/scam2005

SA, DA, Protocols, DR and Security

THANK YOU!