# Supervision systems course

Chapter - 8: SUPERVISORY CONTROL AND DATA ACQUISITION (Prot

*Instructor: Dr.Muath Wahdan*

December 23, 2023

# Outline

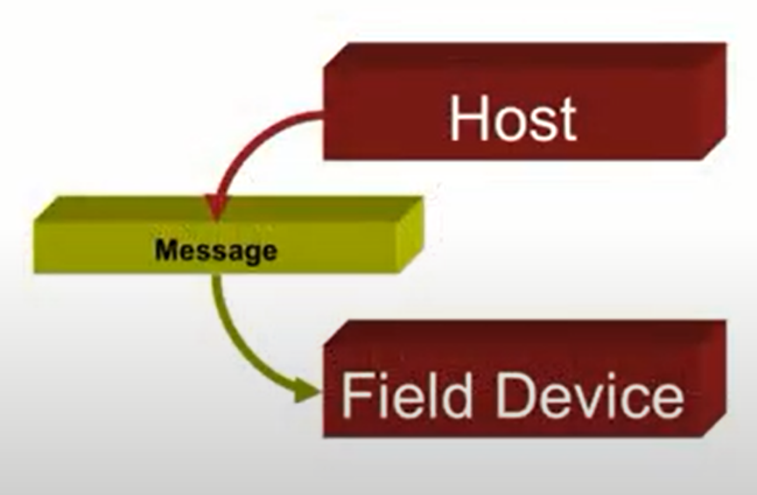
1. Protocols

2. Data Acquisition Strategies

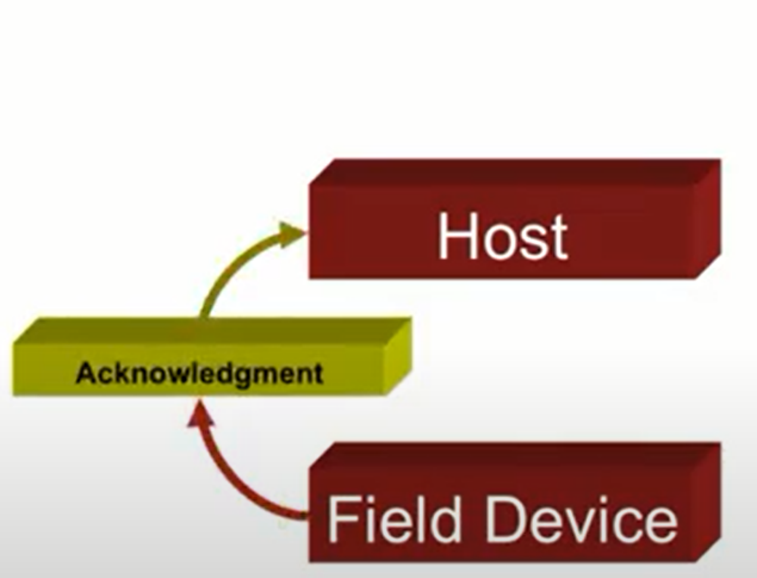
3. Networking Equipment

# Protocol - Handshaking

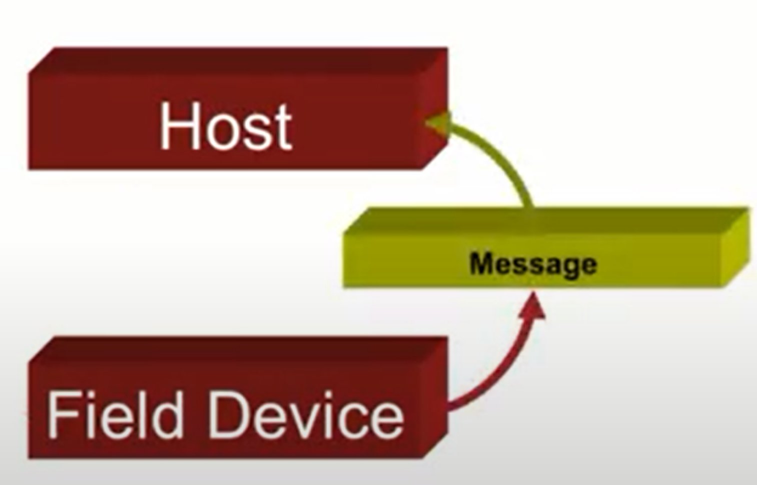
## Handshaking Protocol



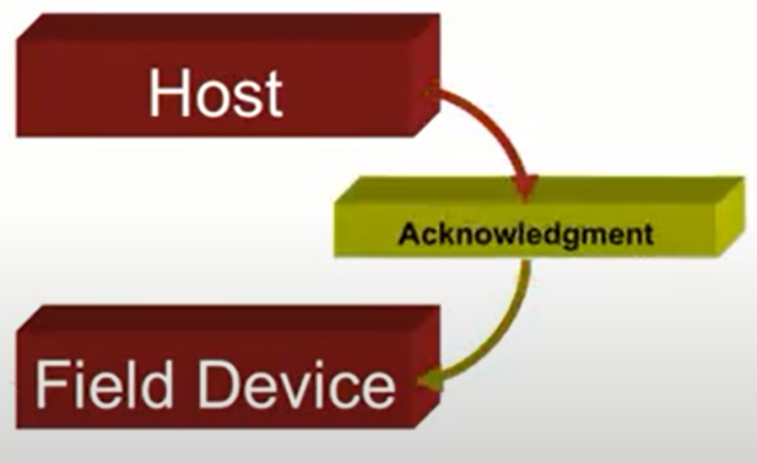
# Protocol - Handshaking



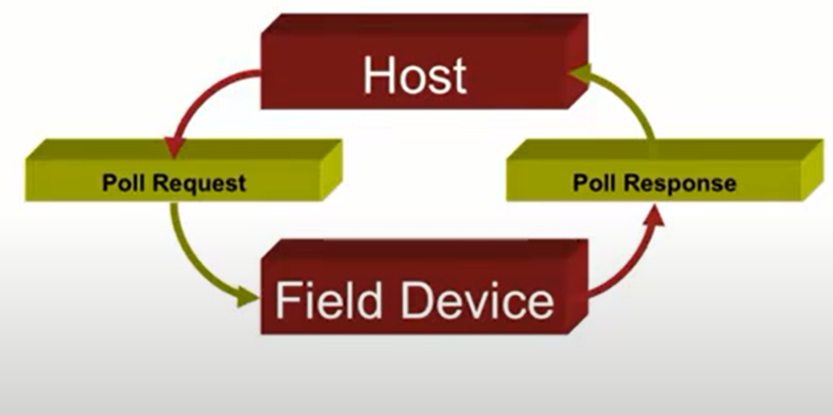
# Protocol - Handshaking



# Protocol - Handshaking



# Protocols - Poll Response



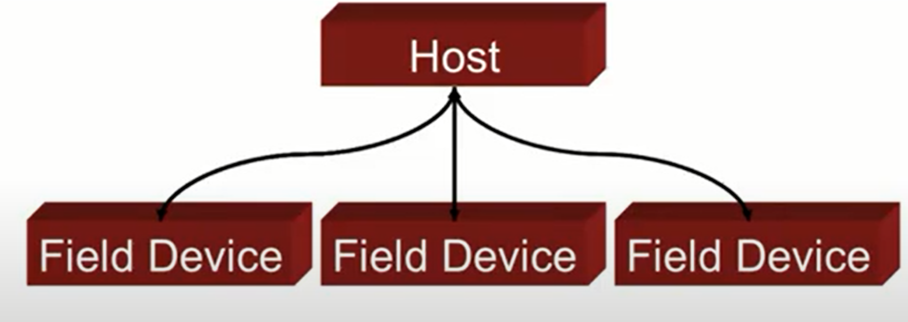
Host

Poll Request

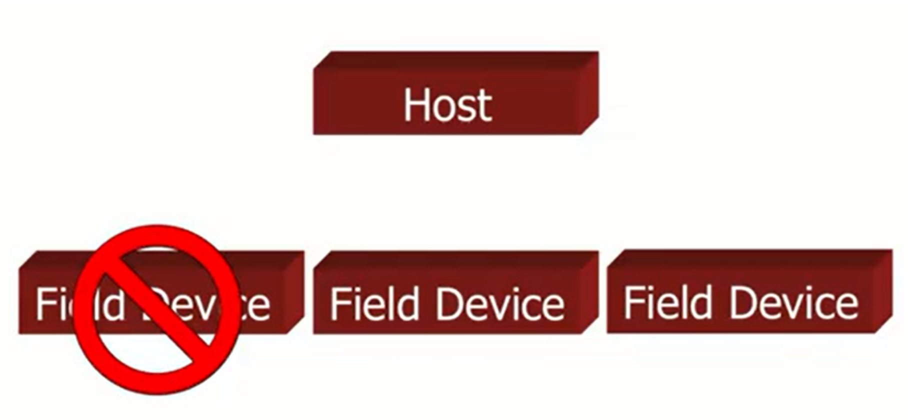
Poll Response

Field Device

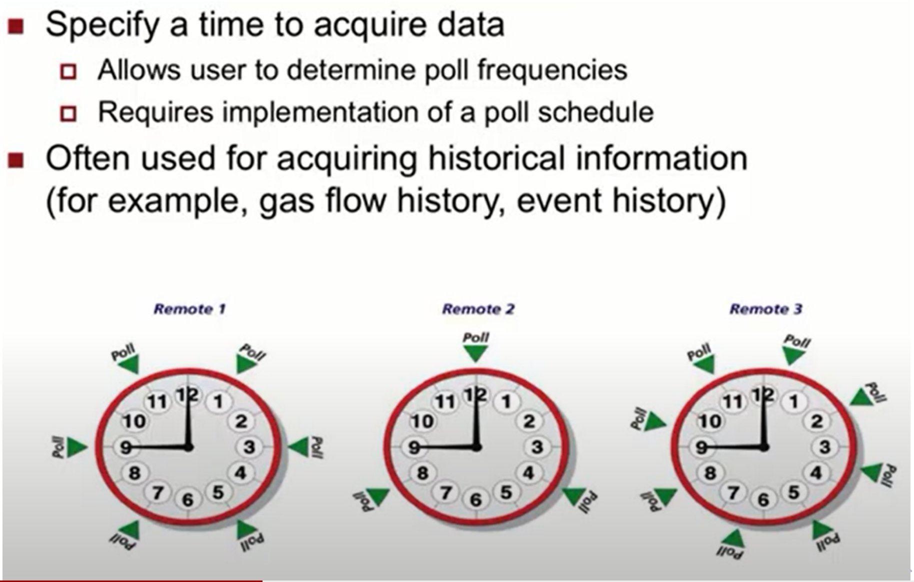
# Round Robin Polling



# Round Robin Polling

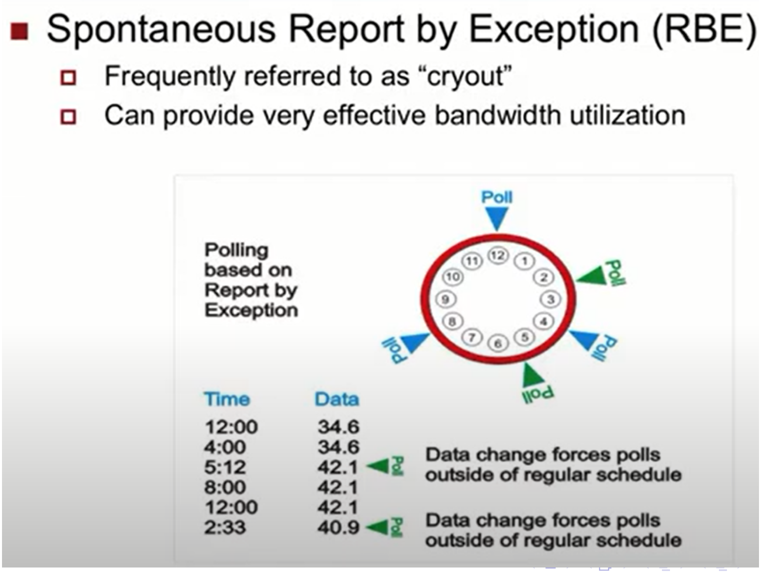


# Timed Polling



- Specify a time to acquire data
  - Allows user to determine poll frequencies
  - Requires implementation of a poll schedule
- Often used for acquiring historical information (for example, gas flow history, event history)

# Data Acquisition Strategies



- Spontaneous Report by Exception (RBE)
  - Frequently referred to as “cryout”
  - Can provide very effective bandwidth utilization

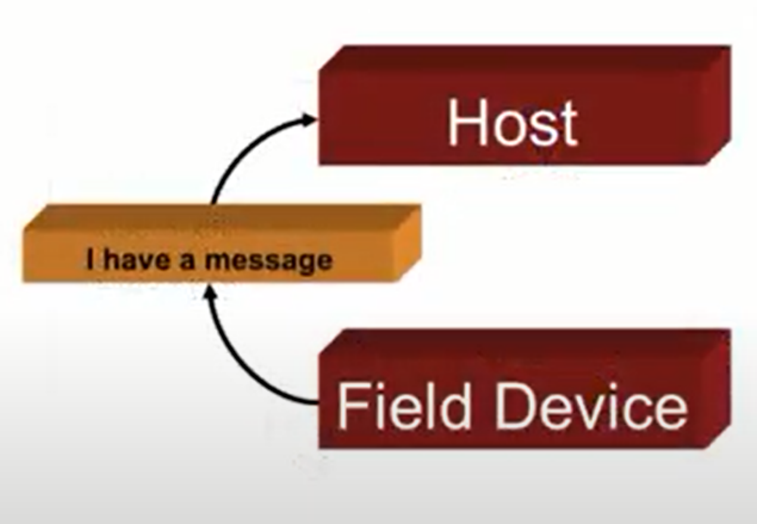
Polling based on Report by Exception

| Time | Data |
|---|---|
| 12:00 | 34.6 |
| 4:00 | 34.6 |
| 5:12 | 42.1 ◀ Poll |
| 8:00 | 42.1 |
| 12:00 | 42.1 |
| 2:33 | 40.9 ◀ Poll |

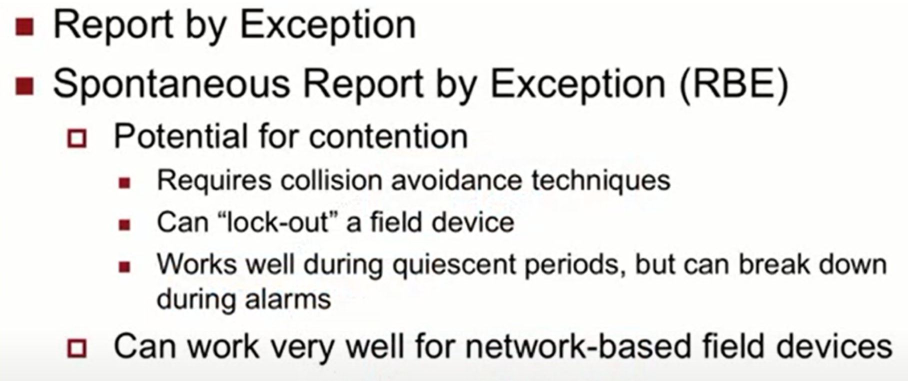
Data change forces polls outside of regular schedule

Data change forces polls outside of regular schedule

# Cry Out

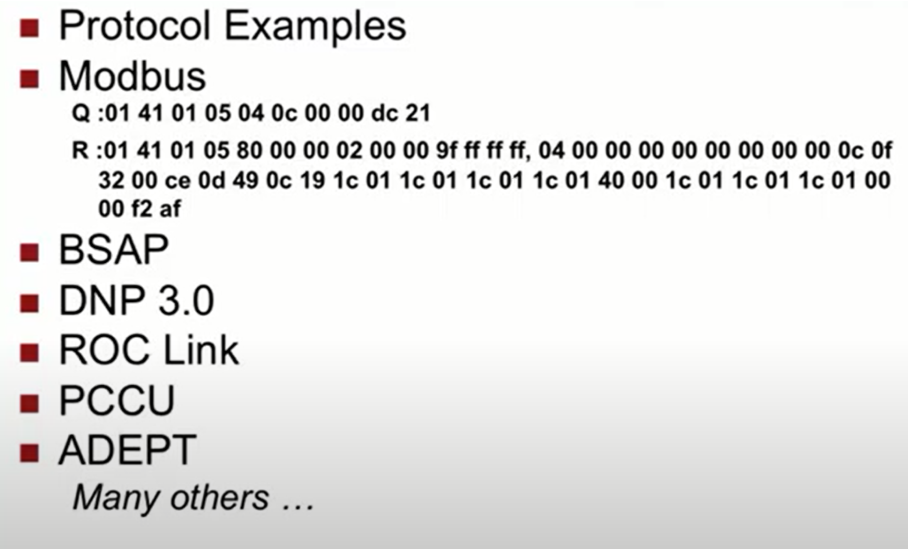


# Report by Exception



- Report by Exception
- Spontaneous Report by Exception (RBE)
  - Potential for contention
    - Requires collision avoidance techniques
    - Can “lock-out” a field device
    - Works well during quiescent periods, but can break down during alarms
  - Can work very well for network-based field devices

# Data Acquisition Strategies



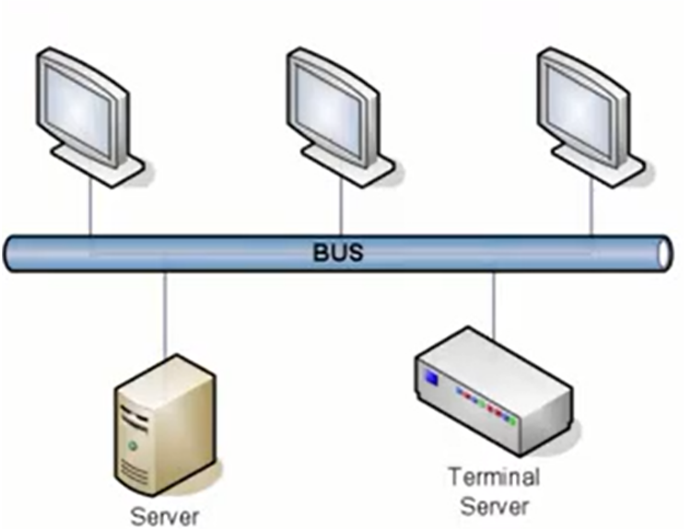
- Protocol Examples
- Modbus

  Q :01 41 01 05 04 0c 00 00 dc 21

  R :01 41 01 05 80 00 00 02 00 00 9f ff ff ff, 04 00 00 00 00 00 00 00 00 0c 0f 32 00 ce 0d 49 0c 19 1c 01 1c 01 1c 01 1c 01 40 00 1c 01 1c 01 1c 01 00 00 f2 af
- BSAP
- DNP 3.0
- ROC Link
- PCCU
- ADEPT

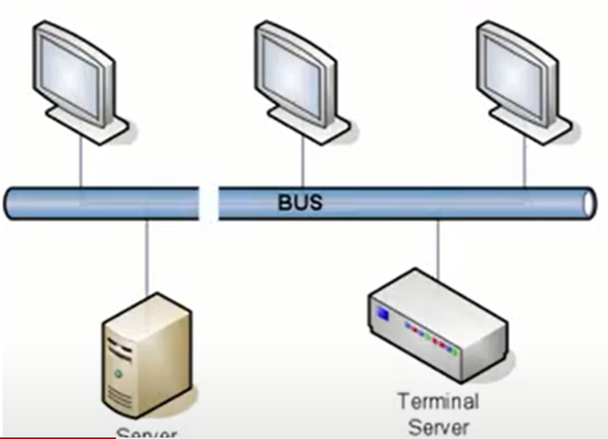
  *Many others …*

# LAN - Bus



# LAN - Bus

If the backbone is broken, the entire segment fails. Bus topologies are relatively easy to install and don't require much cabling compared to the alternatives.

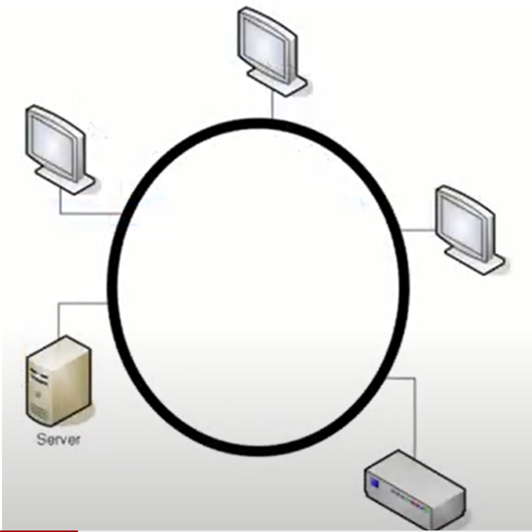


# LAN - Ring

### LAN Ring Topology

A ring topology consists of all computers and other devices that are connected in a loop. Ring topology is also known as a ring network. A ring network can be found in Local Area Networks. In a ring network each node directly connect to two neighbouring nodes. A server may exist in a ring network, but it will not connect to all the nodes in the network. The server, like other nodes, will only communicate to its two neighboring nodes.

# LAN - Ring



# LAN - Ring

### ADVANTAGES OF A RING TOPOLOGY

- Troubleshooting is easy when one of the nodes fails.
- Repair or remove the failing nodes and the network will continue to function.

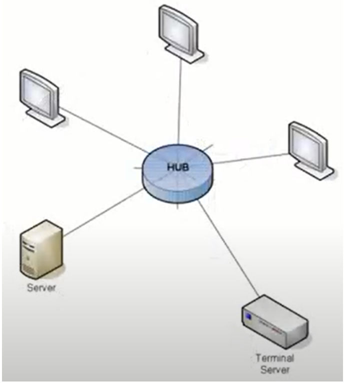
# LAN - Ring

## DISADVANTAGES OF A RING TOPOLOGY

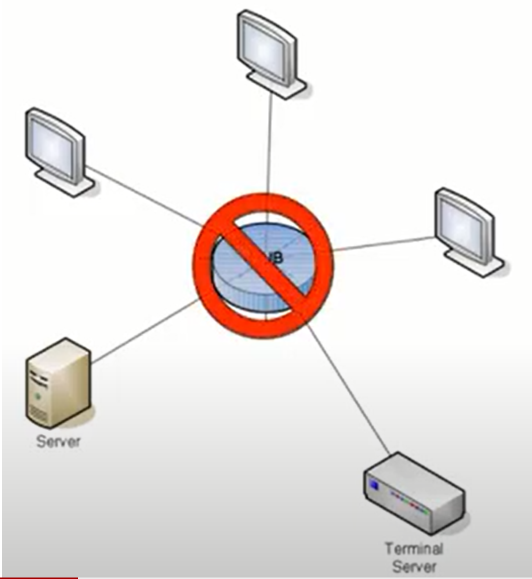
- Implementation is difficult. Network administrator has to terminate the entire network to install a new node between existing nodes.
- A failing node will affect the entire LAN.
- Connecting or removing devices is difficult because network administrator needs to terminate the network in order to do it.
- Network speed decreases when the number of nodes increases. network will continue to function.

# LAN - Hub

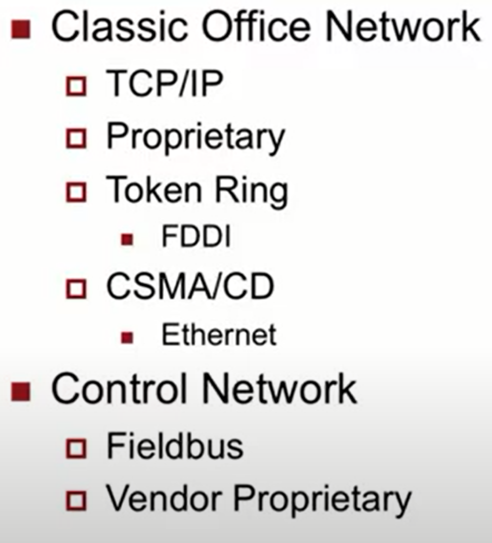
Hubs are a device that cross connects all the wires but hubs unsecure and if the hub dies nothing talks.



# LAN - Hub



# LAN - Protocols

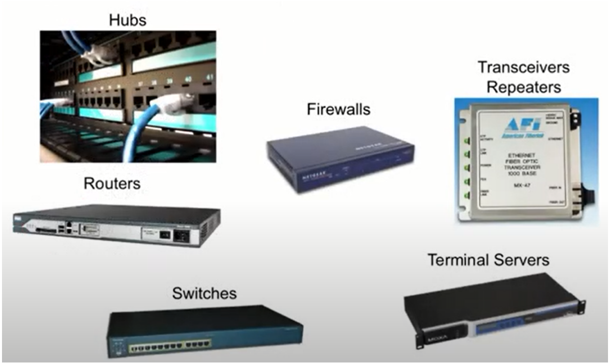


- Classic Office Network
  - TCP/IP
  - Proprietary
  - Token Ring
    - FDDI
  - CSMA/CD
    - Ethernet
- Control Network
  - Fieldbus
  - Vendor Proprietary

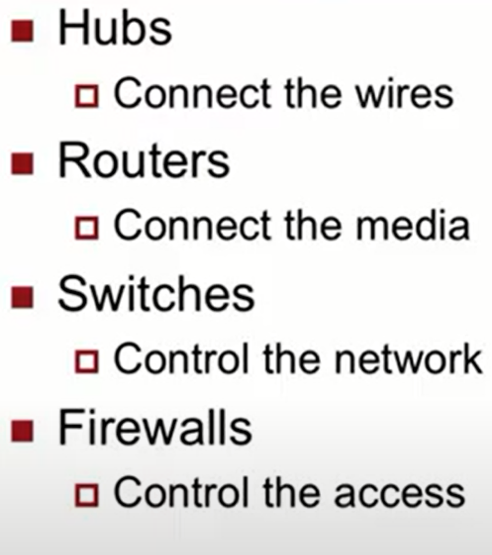
# LAN - Protocols

TCP/IP stands for Transmission Control Protocol/Internet Protocol and is a suite of communication protocols used to interconnect network devices on the internet. TCP/IP is also used as a communications protocol in a private computer network (an intranet or extra-net)

# Networking Equipment



# Networking Equipment

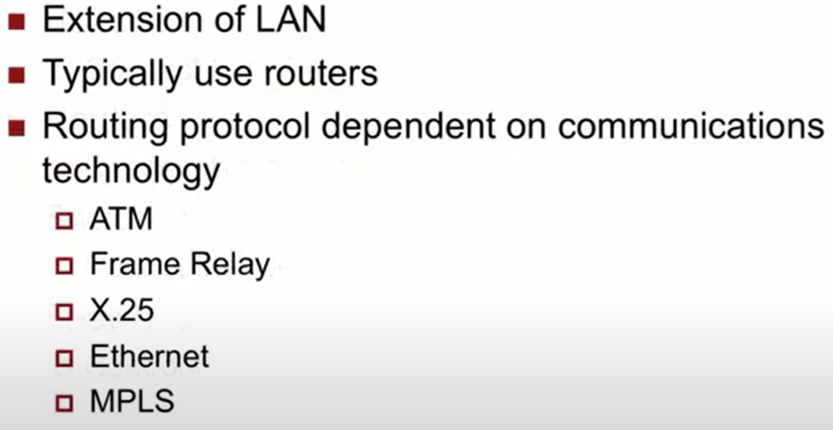


- Hubs
  - Connect the wires
- Routers
  - Connect the media
- Switches
  - Control the network
- Firewalls
  - Control the access

# WAN

A wide area network (WAN) is a telecommunications network that extends over a large geographic area for the primary purpose of computer networking. Probably the most prevalent in the SCADA world are frame Relay and MPLS. frame Relay:dedicated connection between this point and this point and I dont need anybody else to get on my dedicated connection (secure but expensive) MPLS multi-protocol line switching: they give you an access to this point and this point however they switch your traffic based on what bandwidth I have available. (less secure)

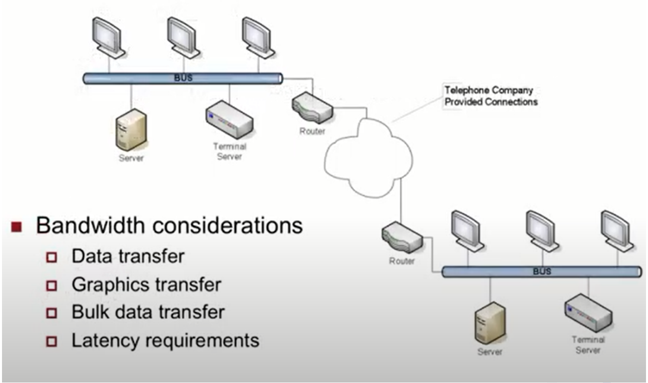
# WAN



- Extension of LAN
- Typically use routers
- Routing protocol dependent on communications technology
  - ATM
  - Frame Relay
  - X.25
  - Ethernet
  - MPLS

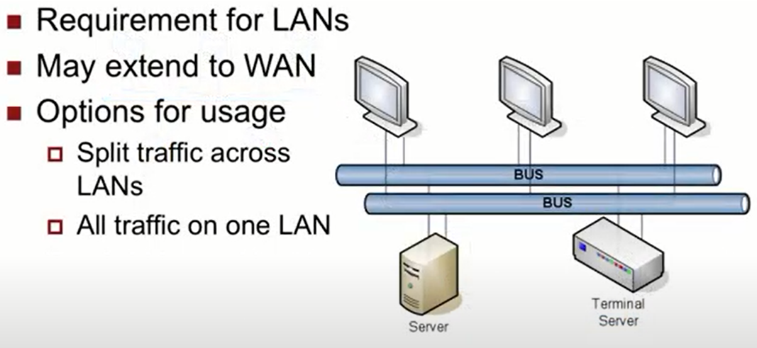
# WAN

This is an example: main control room and remote area and connecting them through a wide area network. Bulk:like videos latency: how long is it ok for controller to wait when they make a request for data until they get the data



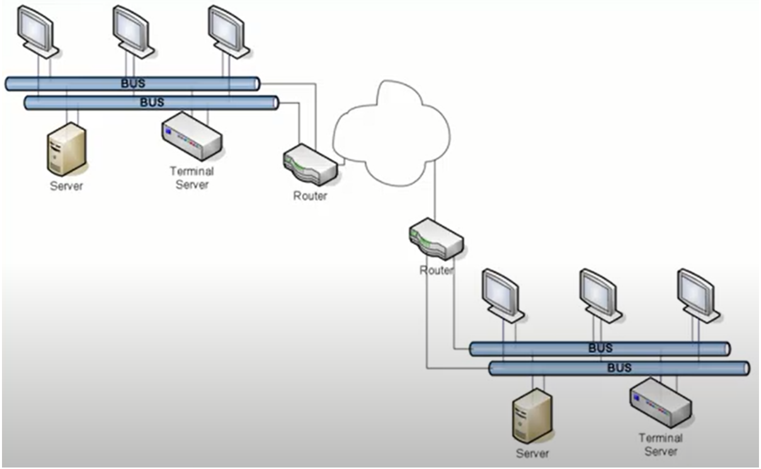
- Bandwidth considerations
  - Data transfer
  - Graphics transfer
  - Bulk data transfer
  - Latency requirements

# Network Redundancy

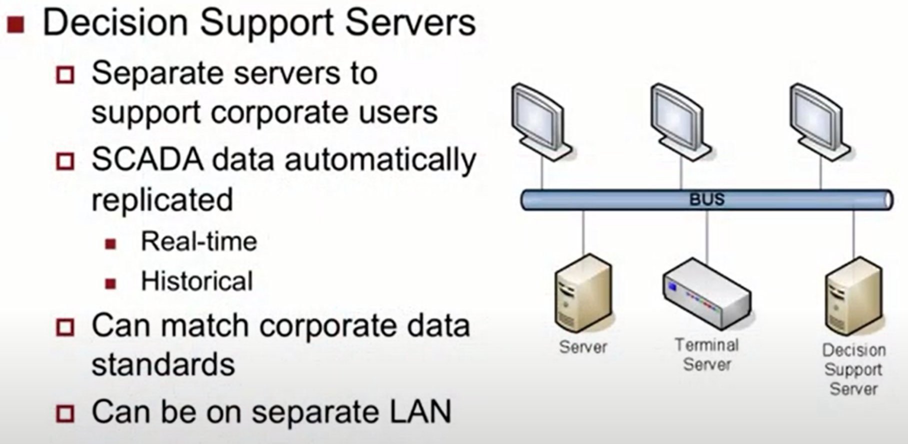


- Requirement for LANs
- May extend to WAN
- Options for usage
  - Split traffic across LANs
  - All traffic on one LAN

# Network Redundancy



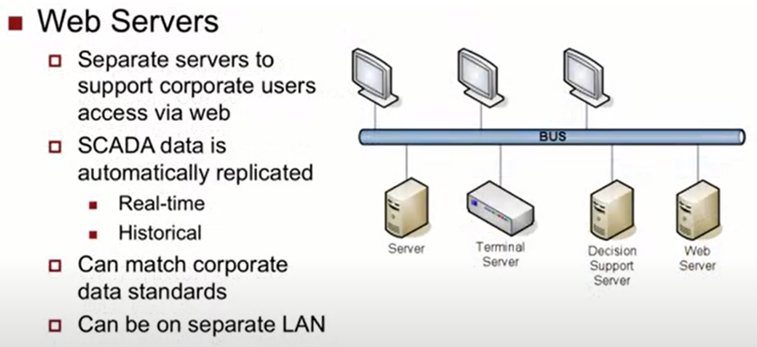
# Corporate System Integration



- Decision Support Servers
  - Separate servers to support corporate users
  - SCADA data automatically replicated
    - Real-time
    - Historical
  - Can match corporate data standards
  - Can be on separate LAN

# Corporate System Integration

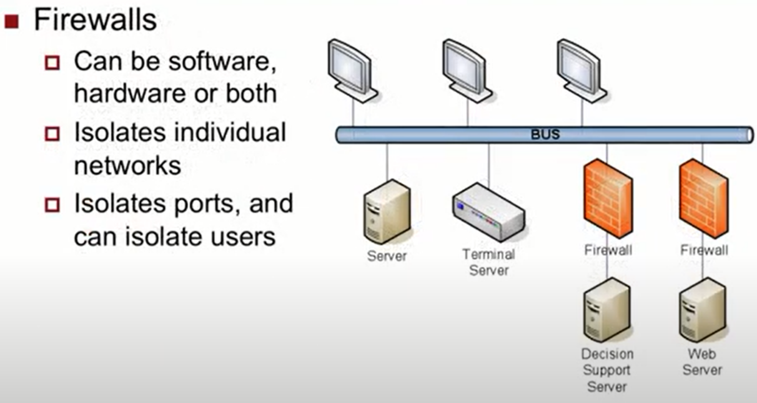
Best way to move data outside the critical user is via web even if thats inside the corporate network most SCADA systems have some kind of web deployment.



- Web Servers
  - Separate servers to support corporate users access via web
  - SCADA data is automatically replicated
    - Real-time
    - Historical
  - Can match corporate data standards
  - Can be on separate LAN

# Corporate System Integration

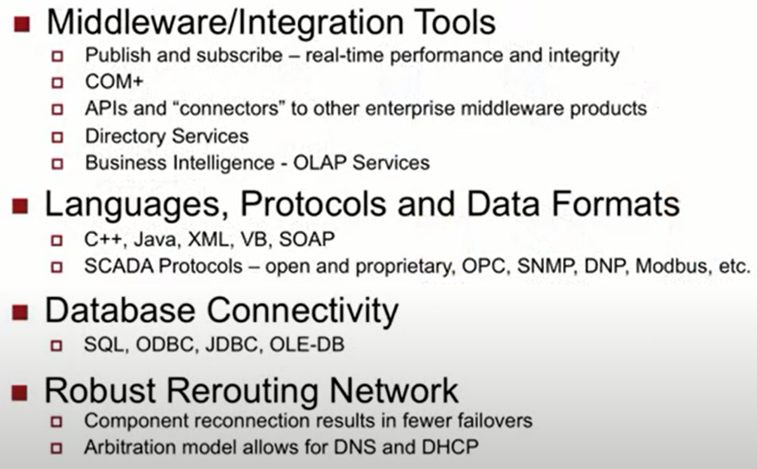
If i’m going to take SCADA data and i’m going to move it to other casual users I probably want to put that data on the other side of a firewall so now what becomes important is whatever software I pick and how it makes its data redundant through a firewall becomes really important



- Firewalls
  - Can be software, hardware or both
  - Isolates individual networks
  - Isolates ports, and can isolate users

# Standards Based Tools

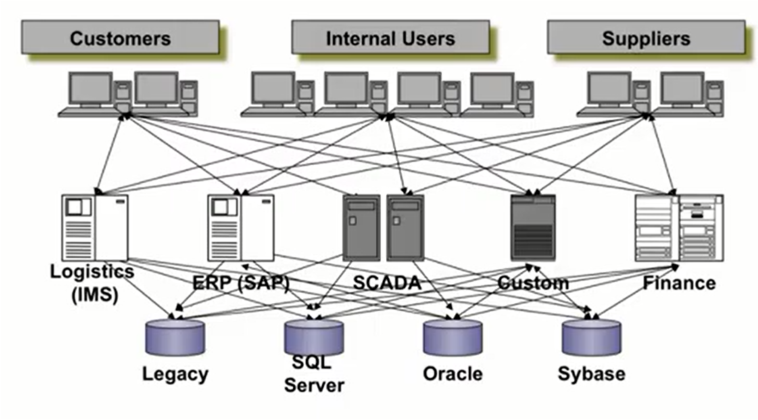
Most of these tools support various kinds of integration....



- Middleware/Integration Tools
  - Publish and subscribe – real-time performance and integrity
  - COM+
  - APIs and "connectors" to other enterprise middleware products
  - Directory Services
  - Business Intelligence - OLAP Services
- Languages, Protocols and Data Formats
  - C++, Java, XML, VB, SOAP
  - SCADA Protocols – open and proprietary, OPC, SNMP, DNP, Modbus, etc.
- Database Connectivity
  - SQL, ODBC, JDBC, OLE-DB
- Robust Rerouting Network
  - Component reconnection results in fewer failovers
  - Arbitration model allows for DNS and DHCP

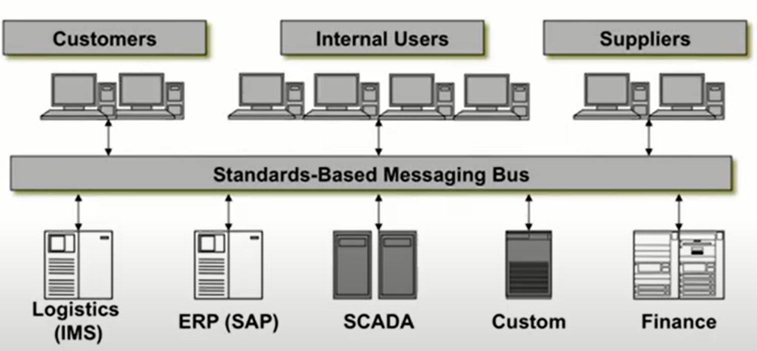
# Corporate System Integration Challenge

Historically SCADA has been Isolated (for cyber security stand point)

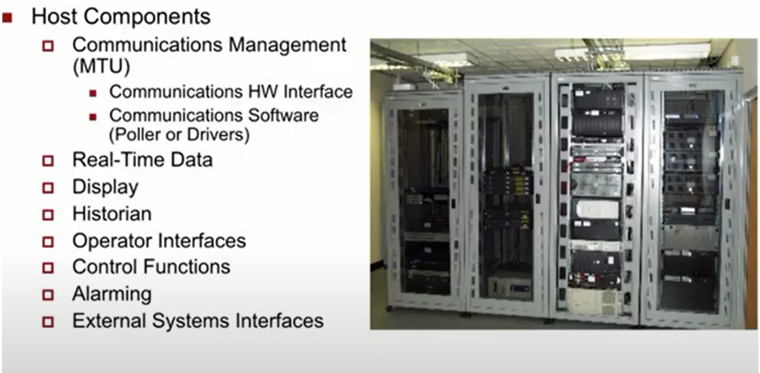


# Corporate System Integration Solution

But we dont need to integrate this scada data there is a lots of people that can use it, logistics, measurement, engineering wants it, all these guys want this data.

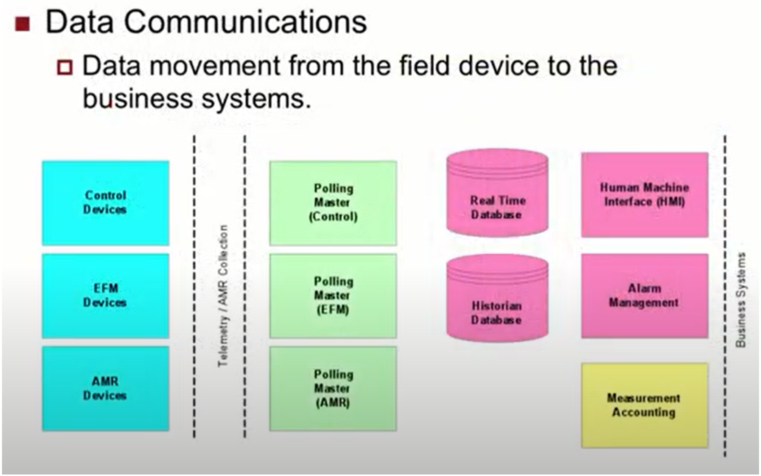


# SCADA Software Components and Interfaces



- Host Components
  - Communications Management (MTU)
    - Communications HW Interface
    - Communications Software (Poller or Drivers)
  - Real-Time Data
  - Display
  - Historian
  - Operator Interfaces
  - Control Functions
  - Alarming
  - External Systems Interfaces

# Some Definitions



- Data Communications
  - Data movement from the field device to the business systems.

Control Devices

EFM Devices

AMR Devices

Telemetry / AMR Collection

Polling Master (Control)

Polling Master (EFM)

Polling Master (AMR)

Real Time Database

Historian Database

Human Machine Interface (HMI)

Alarm Management

Measurement Accounting

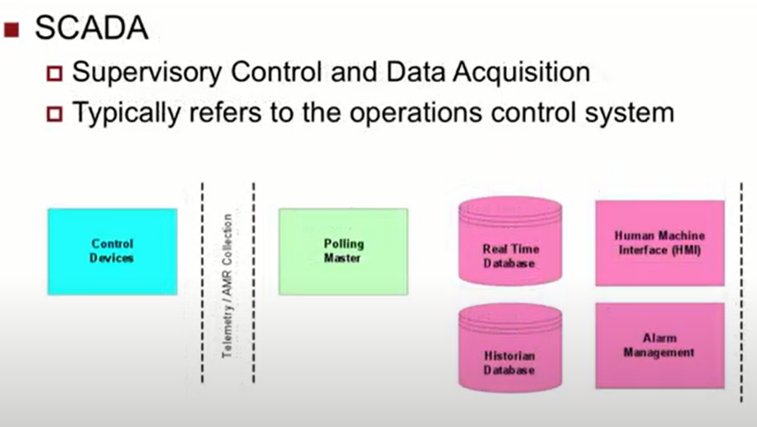
Business Systems

# Some Definitions

These are the standard functions, this is a simple block diagram around a SCADA system so I've got my automation devices in the field or the important part of my SCADA system bcz that what actually controls that's what create the data (real data lives out here), I've got my telemetry I've got my communication software packages, and these are the basic component of my scada system. I've got my real time database gives me the last value that I got the last time I polled every device in my system, so when I request information from the console Im not actually going out to the device and polling, what Im doing is im going to the real time database and showing you what i last got when I polled. the historian keeps an image of every data value I got up to the real-time database. HMI is the package that we use to build all the cool screens with the pretty graphics and the alarm system it's what's monitoring all these values to see if they go outside of bounds and then sending you a notifications.

# Some Definitions

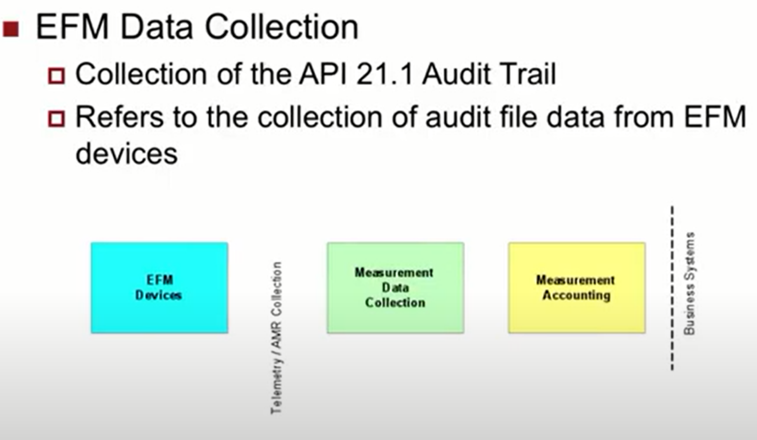
this would be a simple control system ...



- SCADA
  - □ Supervisory Control and Data Acquisition
  - □ Typically refers to the operations control system

# Some Definitions

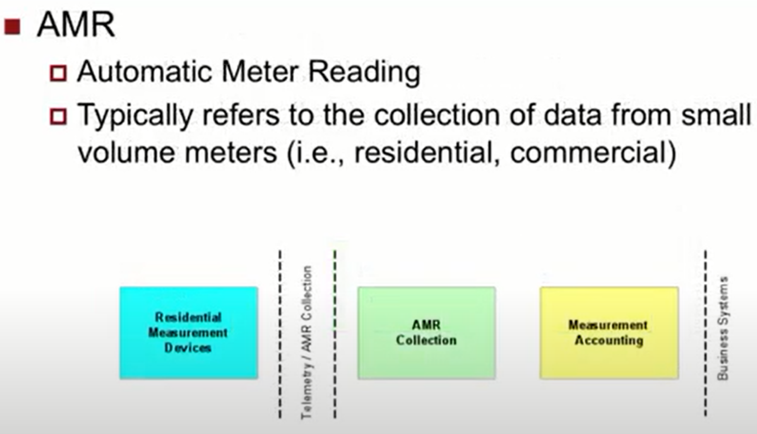
If im just collecting measurment data but im not doing any control im not doing monitoring then i just need these pieces



- EFM Data Collection
  - Collection of the API 21.1 Audit Trail
  - Refers to the collection of audit file data from EFM devices

# Some Definitions

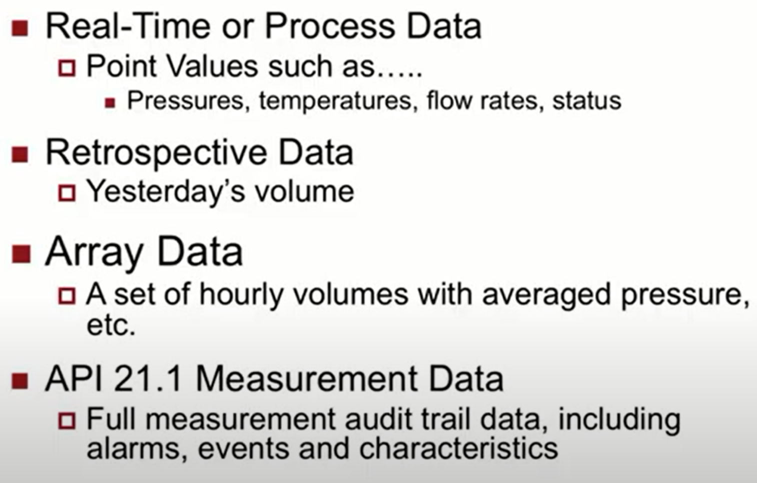
If im doing automatic meter reading so automatic meter reading is residential gas meters residental electric meters



- AMR
  - Automatic Meter Reading
  - Typically refers to the collection of data from small volume meters (i.e., residential, commercial)

# Types of Data

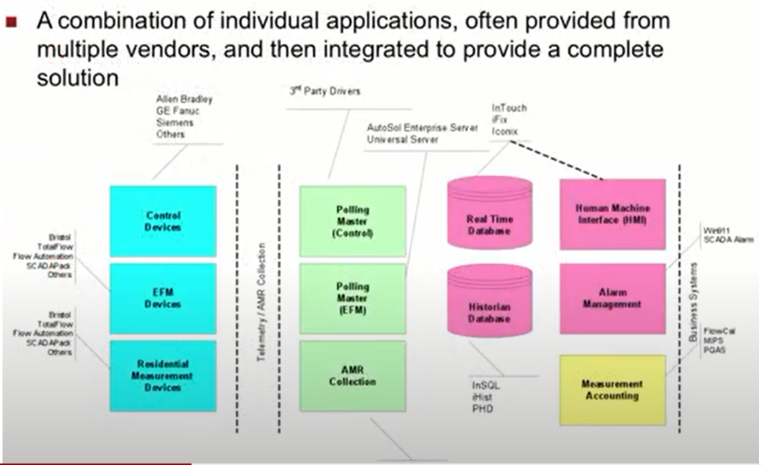
there are 4 types of data that we focus on



- Real-Time or Process Data
  - Point Values such as…..
    - Pressures, temperatures, flow rates, status
- Retrospective Data
  - Yesterday's volume
- Array Data
  - A set of hourly volumes with averaged pressure, etc.
- API 21.1 Measurement Data
  - Full measurement audit trail data, including alarms, events and characteristics

# Typical Implementation-Hybrid

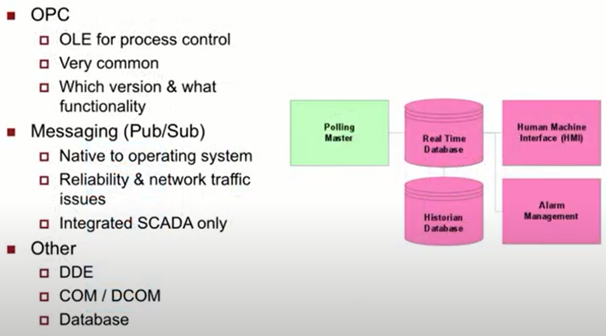
There’s two basic kinds of implementation of SCADA one would be what i would call a hybrid other products cygets a good example it is a monolithic meaning all the feature sets are available in that software package



- A combination of individual applications, often provided from multiple vendors, and then integrated to provide a complete solution

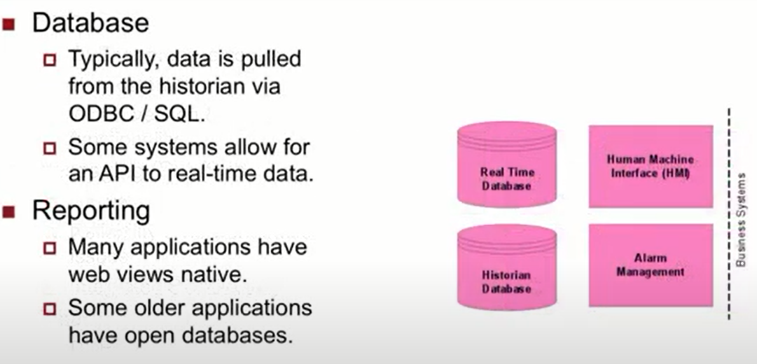
# Hosts-Internal Communications

OPC is ole for process control; it is the primary mechanism for moving real-time data between devices and software applications two kind of OPC: OPC da which OPC data access and its based on windows comdey calm. OPC unified UA which is universal access is the new standard for OPC and it has encryption built in tunneling, security control.



- OPC
  - OLE for process control
  - Very common
  - Which version & what functionality
- Messaging (Pub/Sub)
  - Native to operating system
  - Reliability & network traffic issues
  - Integrated SCADA only
- Other
  - DDE
  - COM / DCOM
  - Database

# Hosts-External Communications



- Database
  - Typically, data is pulled from the historian via ODBC / SQL.
  - Some systems allow for an API to real-time data.
- Reporting
  - Many applications have web views native.
  - Some older applications have open databases.

Real Time Database

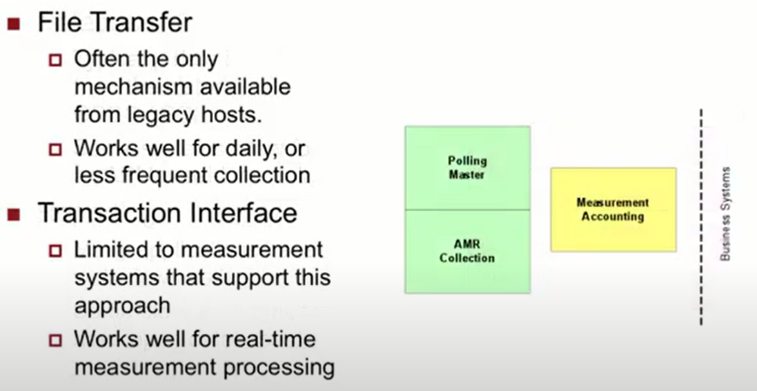
Human Machine Interface (HMI)

Historian Database

Alarm Management

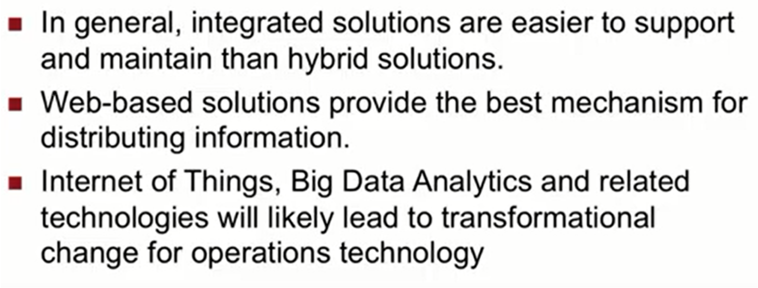
Business Systems

# Hosts-Communications to Measurement System



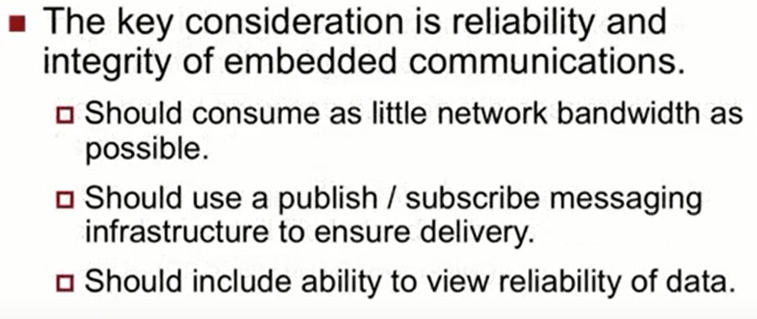
- File Transfer
  - Often the only mechanism available from legacy hosts.
  - Works well for daily, or less frequent collection
- Transaction Interface
  - Limited to measurement systems that support this approach
  - Works well for real-time measurement processing

# Observations



- In general, integrated solutions are easier to support and maintain than hybrid solutions.
- Web-based solutions provide the best mechanism for distributing information.
- Internet of Things, Big Data Analytics and related technologies will likely lead to transformational change for operations technology

# Observations

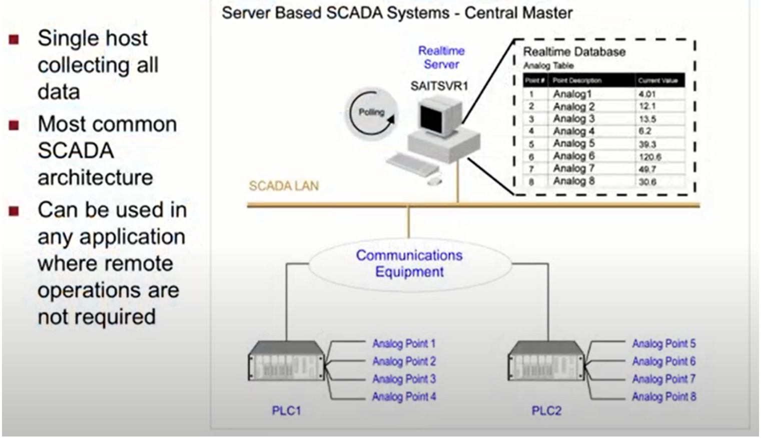


- The key consideration is reliability and integrity of embedded communications.
  - Should consume as little network bandwidth as possible.
  - Should use a publish / subscribe messaging infrastructure to ensure delivery.
  - Should include ability to view reliability of data.

# Central Master

All SCADA systems are client-server, the polling engine is the server. So the client (HMI) asks the polling engine for the data and the polling engine goes out and gets it if it's a demand request otherwise the server is asking for the data and bring it up and storing it in the HMI. e.g. simple SCADA is a central master and HMI package sitting on top of it.

# Central Master



- Single host collecting all data
- Most common SCADA architecture
- Can be used in any application where remote operations are not required

Server Based SCADA Systems - Central Master

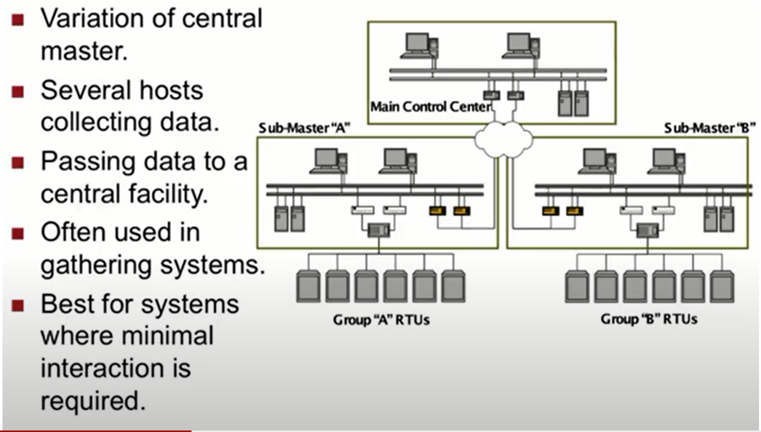
Realtime Database

Analog Table

| Point # | Point Description | Current Value |
|---|---|---|
| 1 | Analog1 | 4.01 |
| 2 | Analog 2 | 12.1 |
| 3 | Analog 3 | 13.5 |
| 4 | Analog 4 | 6.2 |
| 5 | Analog 5 | 39.3 |
| 6 | Analog 6 | 120.6 |
| 7 | Analog 7 | 49.7 |
| 8 | Analog 8 | 30.6 |

# Distributed System - Peer to Peer

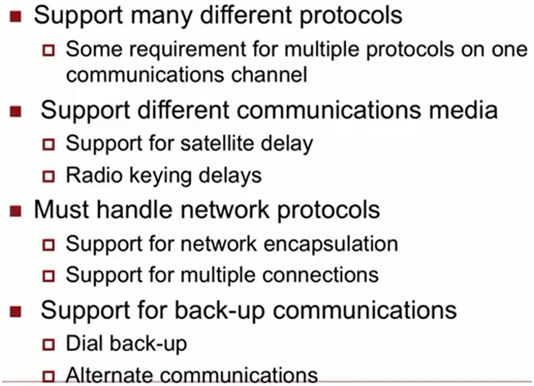
The next kind of system would be what would be called a distributed system or a peer-to-peer Signet is a distributed system bcz I can have its polling server in multiple locations through out my business and any of the HMIs have connectivity can see any one of those polling servers



- Variation of central master.
- Several hosts collecting data.
- Passing data to a central facility.
- Often used in gathering systems.
- Best for systems where minimal interaction is required.

# Polling Module Requirements

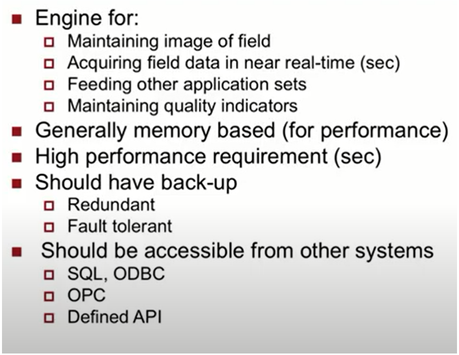
Polling module it's one of the most critical pieces of the system it needs to be able to handle multiple protocols, support multiple media,primary polling path and secondary polling paths,.....



- Support many different protocols
  - Some requirement for multiple protocols on one communications channel
- Support different communications media
  - Support for satellite delay
  - Radio keying delays
- Must handle network protocols
  - Support for network encapsulation
  - Support for multiple connections
- Support for back-up communications
  - Dial back-up
  - Alternate communications

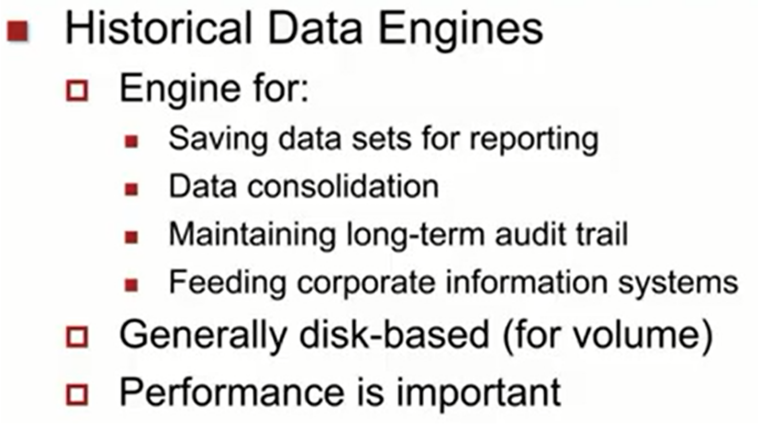
# Real-Time Data Engine

Historical data Engines its constrained mostly by disk volume it need algorithm for data reduction real-time data engine I got an image of the real-time data it's where I'll feed other applications that need to see the real time data (for real data they run the applications on the RAM of the server so it's fast)



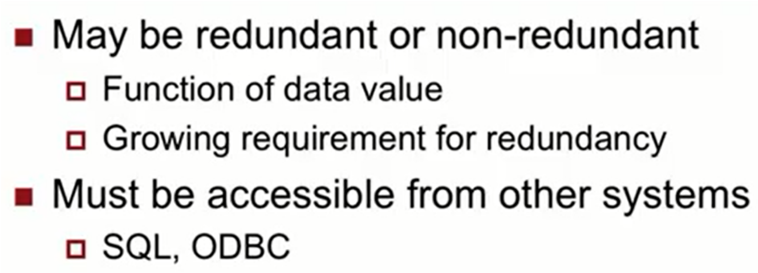
- Engine for:
  - Maintaining image of field
  - Acquiring field data in near real-time (sec)
  - Feeding other application sets
  - Maintaining quality indicators
- Generally memory based (for performance)
- High performance requirement (sec)
- Should have back-up
  - Redundant
  - Fault tolerant
- Should be accessible from other systems
  - SQL, ODBC
  - OPC
  - Defined API

# Host Systems



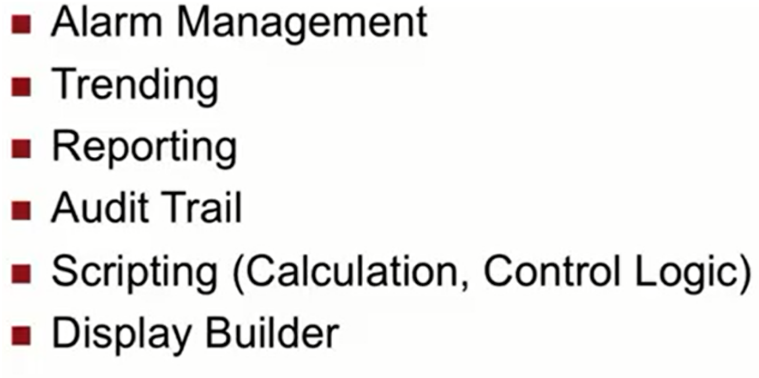
- Historical Data Engines
  - Engine for:
    - Saving data sets for reporting
    - Data consolidation
    - Maintaining long-term audit trail
    - Feeding corporate information systems
  - Generally disk-based (for volume)
  - Performance is important

# Historian



- May be redundant or non-redundant
  - Function of data value
  - Growing requirement for redundancy
- Must be accessible from other systems
  - SQL, ODBC

## SCADA Core Components

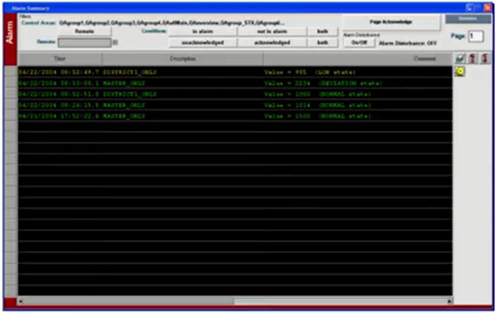


- Alarm Management
- Trending
- Reporting
- Audit Trail
- Scripting (Calculation, Control Logic)
- Display Builder

# Alarm Management

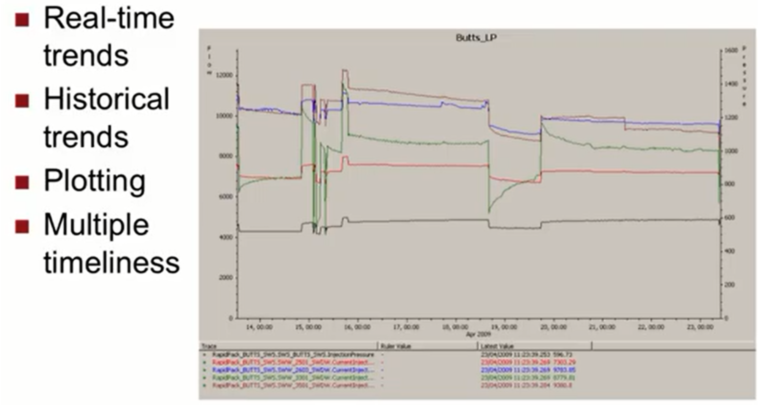
.... give the highest priority for the alarm....

- Alarm management
- Routing
- Priority
- Acknowledgment
- Filtering
- Suppressing
- Operational context



```
04/22/2004 08:52:49.7 DISTRICT1_ONLY        Value = 985   (LOW state)
04/22/2004 08:53:00.1 MASTER_ONLY           Value = 2234  (DEVIATION state)
04/22/2004 08:52:51.0 DISTRICT1_ONLY        Value = 1000  (NORMAL state)
04/22/2004 08:26:15.5 MASTER_ONLY           Value = 1014  (NORMAL state)
04/21/2004 17:52:22.6 MASTER_ONLY           Value = 1500  (NORMAL state)
```

# Trending

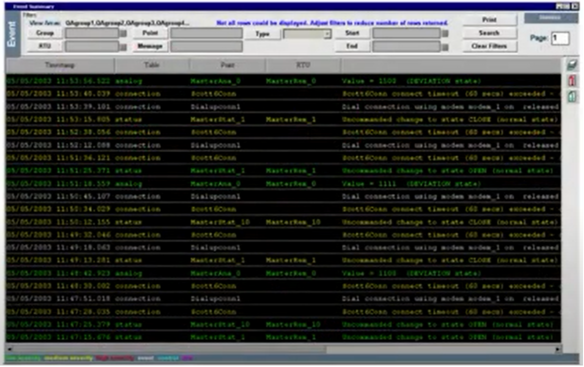


- Real-time trends
- Historical trends
- Plotting
- Multiple timeliness

| Trace | Ruler Value | Latest Value |
|---|---|---|
| RapidPack_BUTTS_SWS.SWS_BUTTS_SWS.InjectionPressure | - | 23/04/2009 11:23:39.253 596.73 |
| RapidPack_BUTTS_SWS.SWW_2501_SWDW.CurrentInject... | - | 23/04/2009 11:23:39.269 7303.29 |
| RapidPack_BUTTS_SWS.SWW_2601_SWDW.CurrentInject... | - | 23/04/2009 11:23:39.269 9783.85 |
| RapidPack_BUTTS_SWS.SWW_3301_SWDW.CurrentInject... | - | 23/04/2009 11:23:39.269 6779.81 |
| RapidPack_BUTTS_SWS.SWW_3501_SWDW.CurrentInject... | - | 23/04/2009 11:23:39.284 9380.8 |

# Audit Trail

- Typically an events package
- Tracks system actions
- Tracks operator actions



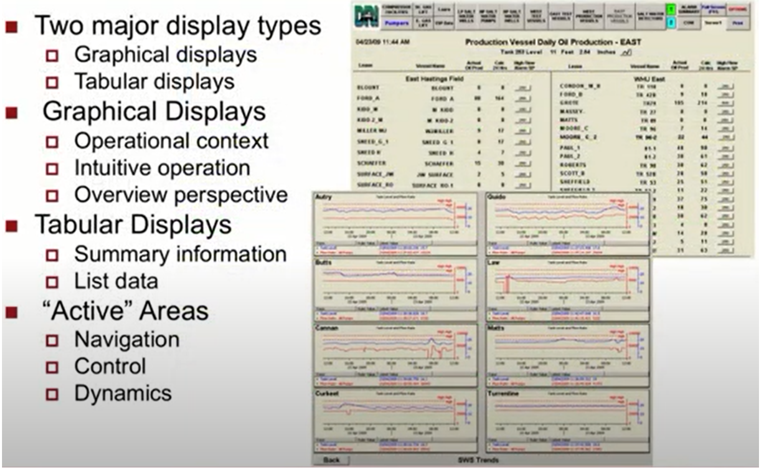
View Areas: QAgroup1,QAgroup2,QAgroup3,QAgroup4...

Not all rows could be displayed. Adjust filters to reduce number of rows returned.

Page: 1

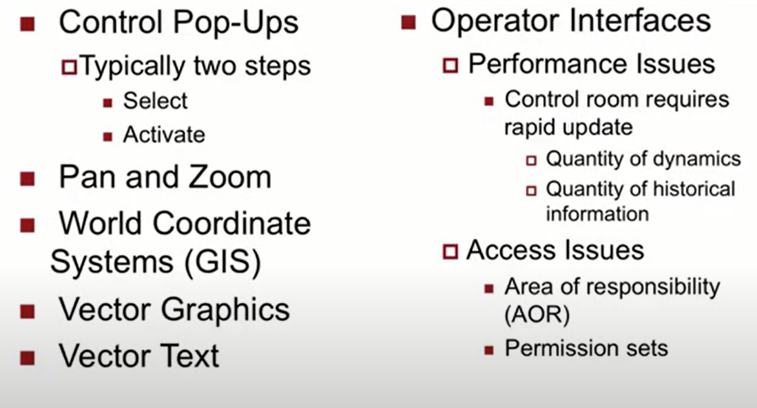
```
Timestamp               Table       Point          RTU
05/05/2003 11:53:56.522 analog      MasterAna_0    MasterRem_0   Value = 1100  (DEVIATION state)
05/05/2003 11:53:40.039 connection  Scott6Conn                   Scott6Conn connect timeout (60 secs) exceeded -
05/05/2003 11:53:39.101 connection  Dialupconn1                  Dial connection using modem modem_1 on  released
05/05/2003 11:53:15.805 status      MasterStat_1   MasterRem_1   Uncommanded change to state CLOSE (normal state)
05/05/2003 11:52:38.056 connection  Scott6Conn                   Scott6Conn connect timeout (60 secs) exceeded -
05/05/2003 11:52:12.088 connection  Dialupconn1                  Dial connection using modem modem_1 on  released
05/05/2003 11:51:36.121 connection  Scott6Conn                   Scott6Conn connect timeout (60 secs) exceeded -
05/05/2003 11:51:25.371 status      MasterStat_1   MasterRem_1   Uncommanded change to state OPEN (normal state)
05/05/2003 11:51:18.559 analog      MasterAna_0    MasterRem_0   Value = 1111  (DEVIATION state)
05/05/2003 11:50:45.107 connection  Dialupconn1                  Dial connection using modem modem_1 on  released
05/05/2003 11:50:34.029 connection  Scott6Conn                   Scott6Conn connect timeout (60 secs) exceeded -
05/05/2003 11:50:12.155 status      MasterStat_10  MasterRem_10  Uncommanded change to state CLOSE (normal state)
05/05/2003 11:49:32.046 connection  Scott6Conn                   Scott6Conn connect timeout (60 secs) exceeded -
05/05/2003 11:49:18.063 connection  Dialupconn1                  Dial connection using modem modem_1 on  released
05/05/2003 11:49:13.281 status      MasterStat_1   MasterRem_1   Uncommanded change to state CLOSE (normal state)
05/05/2003 11:48:42.923 analog      MasterAna_0    MasterRem_0   Value = 1100  (DEVIATION state)
05/05/2003 11:48:39.002 connection  Scott6Conn                   Scott6Conn connect timeout (60 secs) exceeded -
05/05/2003 11:47:51.018 connection  Dialupconn1                  Dial connection using modem modem_1 on  released
05/05/2003 11:47:28.035 connection  Scott6Conn                   Scott6Conn connect timeout (60 secs) exceeded -
05/05/2003 11:47:25.379 status      MasterStat_10  MasterRem_10  Uncommanded change to state OPEN (normal state)
05/05/2003 11:47:15.676 status      MasterStat_1   MasterRem_1   Uncommanded change to state OPEN (normal state)
```

# Displays



- Two major display types
  - Graphical displays
  - Tabular displays
- Graphical Displays
  - Operational context
  - Intuitive operation
  - Overview perspective
- Tabular Displays
  - Summary information
  - List data
- “Active” Areas
  - Navigation
  - Control
  - Dynamics

# Displays1



- Control Pop-Ups
  - Typically two steps
    - Select
    - Activate
- Pan and Zoom
- World Coordinate Systems (GIS)
- Vector Graphics
- Vector Text

- Operator Interfaces
  - Performance Issues
    - Control room requires rapid update
      - Quantity of dynamics
      - Quantity of historical information
  - Access Issues
    - Area of responsibility (AOR)
    - Permission sets

# Thank You!