SCADA
ARCHITECTURE
(continued)

SYSTEM ARCHITECTURE

Element	Function
RTU/IED or PLC	Electronic communication, Data acquisition (DAQ), Monitoring, Control
Master Controller	Data collection, Calculation,Report generation
Human Machine Interface	Allows human operators to monitor and control the system
Historian	Data collection, storage and retrieval
Communication Network	Electronic communication and security

SCADA - ARCHITECTURE

ALGONQUIN COLLEGE

SYSTEM ARCHITECTURE

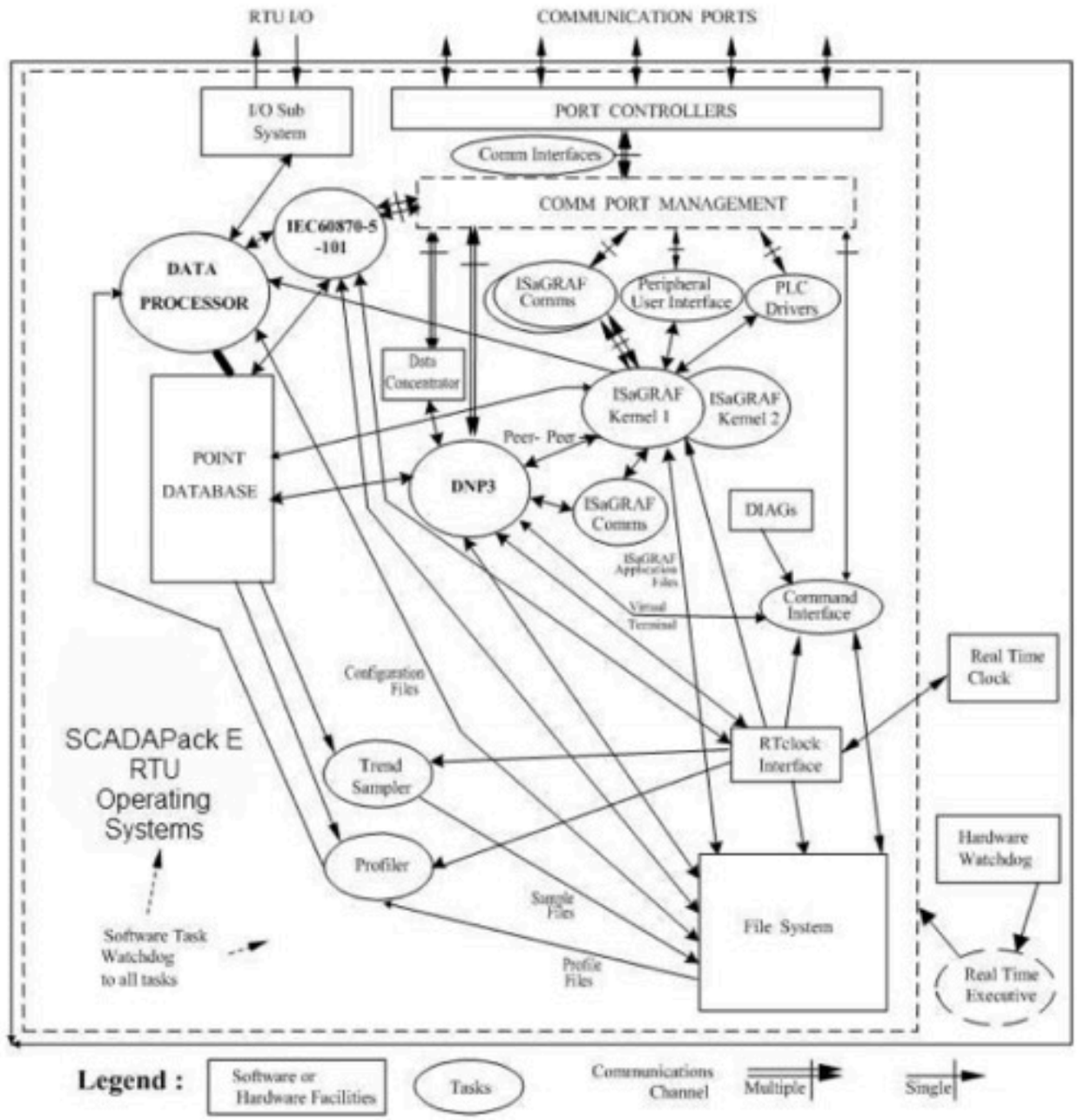
RTU - Remote Terminal Unit

SCADA - ARCHITECTURE

ALGONQUIN COLLEGE

SYSTEM ARCHITECTURE

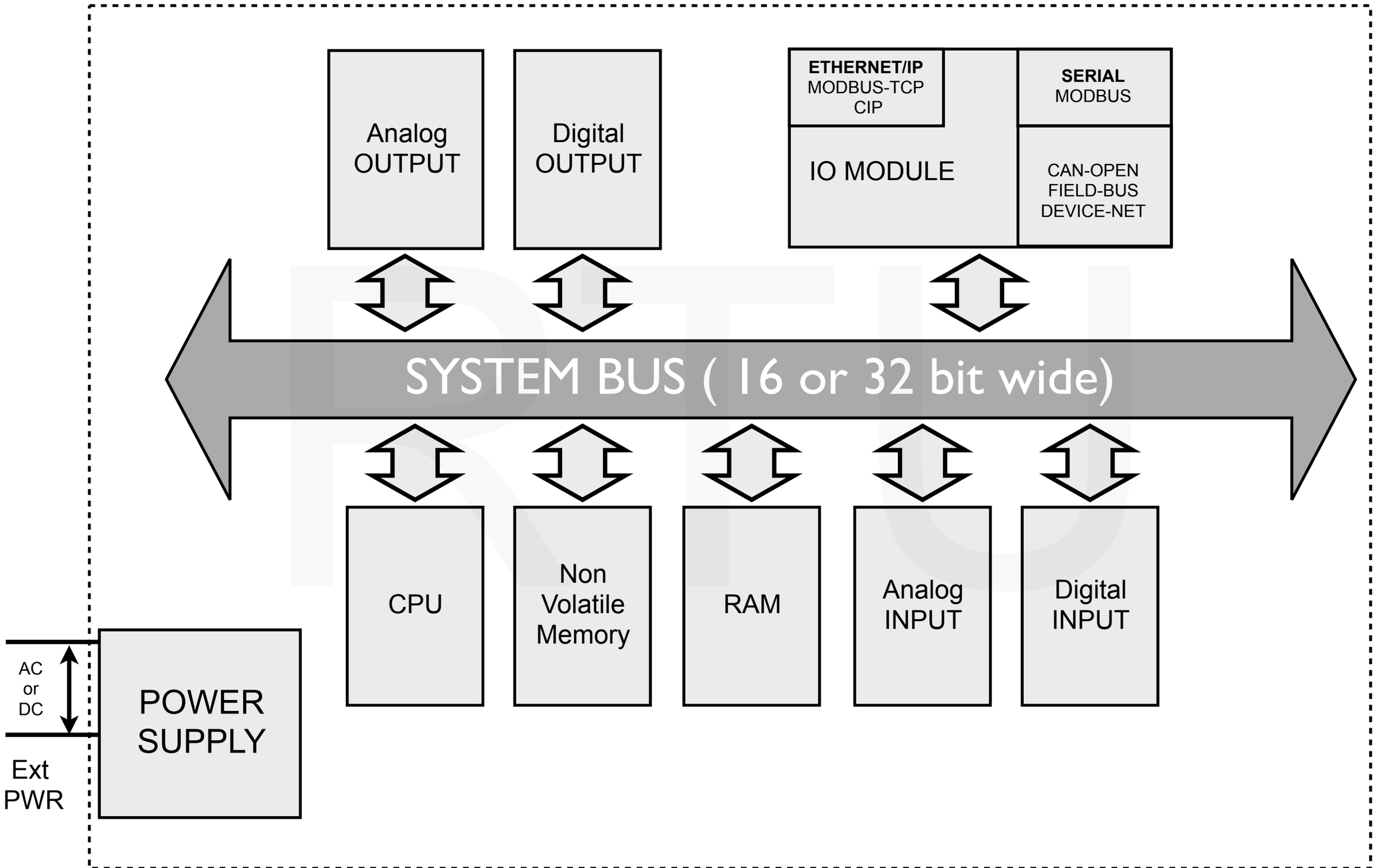
RTU - Remote Terminal Unit



SCADA - ARCHITECTURE

ALGONQUIN COLLEGE

Remote Terminal Unit



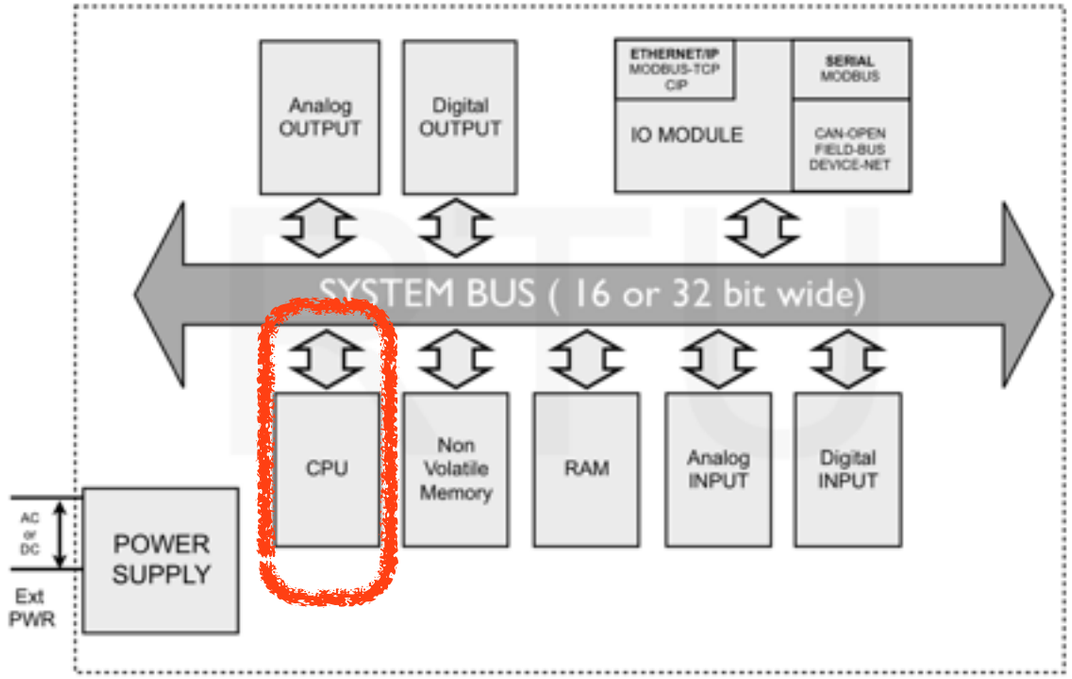
SCADA - ARCHITECTURE

ALGONQUIN COLLEGE

Remote Terminal Unit

CPU

- Based on OEM microprocessor
- ARM , Atmel, Intel
- Used to be 16 bit, now 32 bit, future 64 bit
- Harvard vs Von Neumann
- Most micros are now Big Endian
- ARM now allows you to configure endianness
- Power efficiency becoming a selling feature
- Clock speeds are in GHz or high MHz
- Usually contain the system timers



https://en.wikipedia.org/wiki/Microprocessor

https://en.wikipedia.org/wiki/Computer_architecture

https://en.wikipedia.org/wiki/Endianness

https://en.wikipedia.org/wiki/Harvard_architecture

https://en.wikipedia.org/wiki/Von_Neumann_architecture

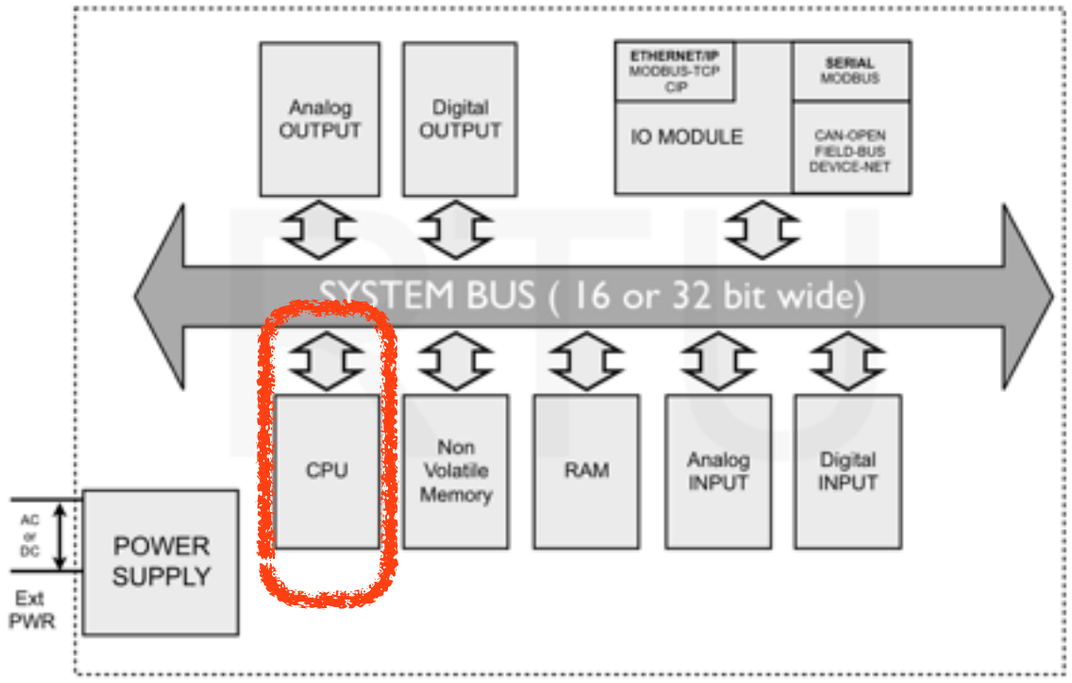
https://en.wikipedia.org/wiki/Modified_Harvard_architecture

SCADA - ARCHITECTURE

ALGONQUIN COLLEGE

Remote Terminal Unit

CPU



Runs custom low level firmware

Firmware safety has many standards

Standards map to specific industry

IEC 61508 is for the electrical power industry

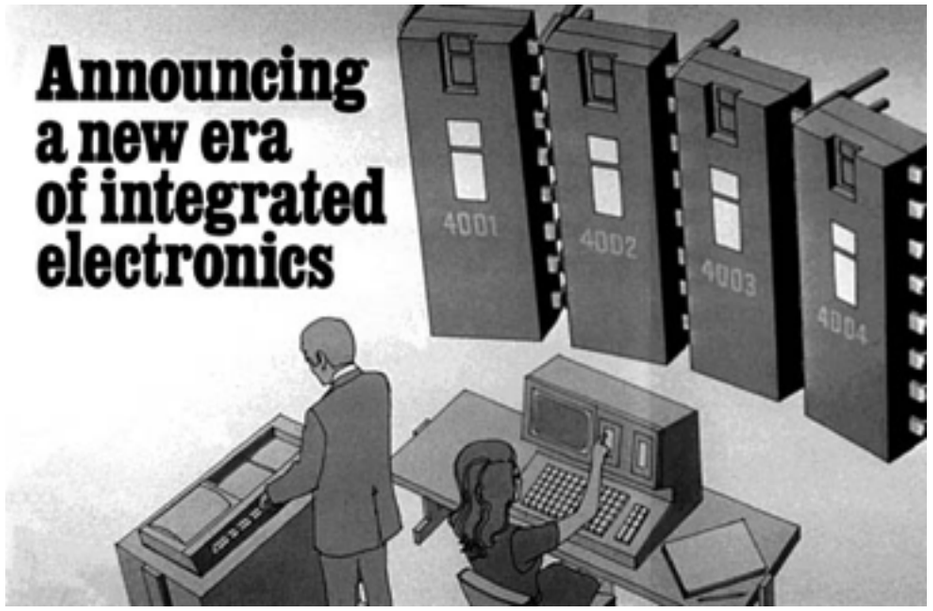
https://en.wikipedia.org/wiki/Software_system_safety

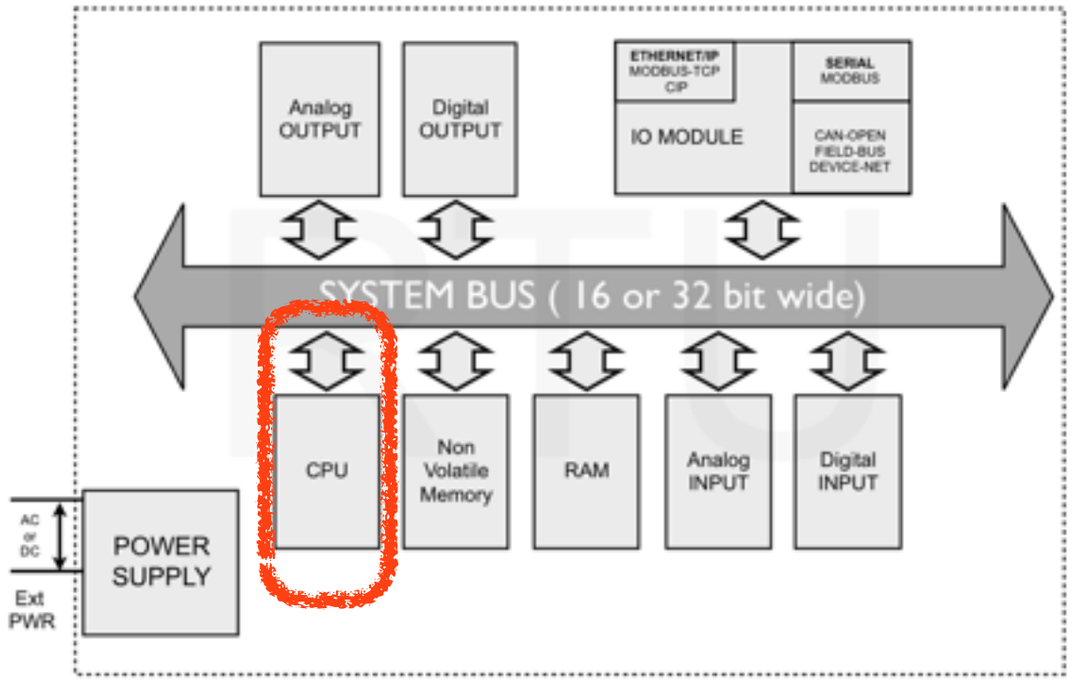
https://en.wikipedia.org/wiki/Software_assurance

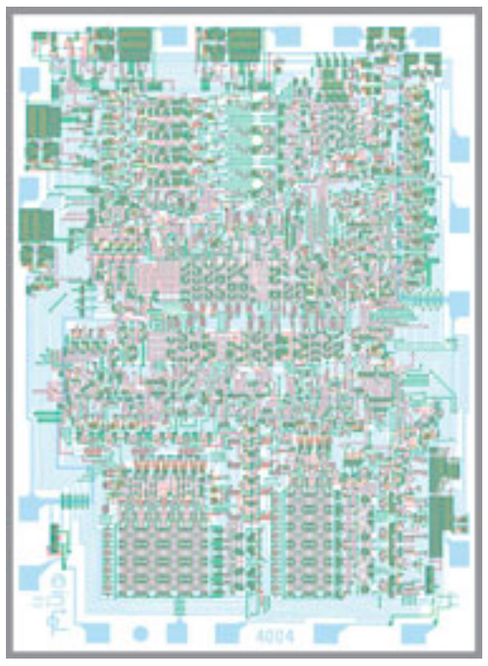
https://en.wikipedia.org/wiki/IEC_61508

Remote Terminal Unit

CPU







INTEL 4004

4 Bit Microprocessor

Originally designed for a calculator company in Japan

https://en.wikipedia.org/wiki/Intel_4004

https://www.youtube.com/watch?v=j00AULJLCNo

Remote Terminal Unit

CPU

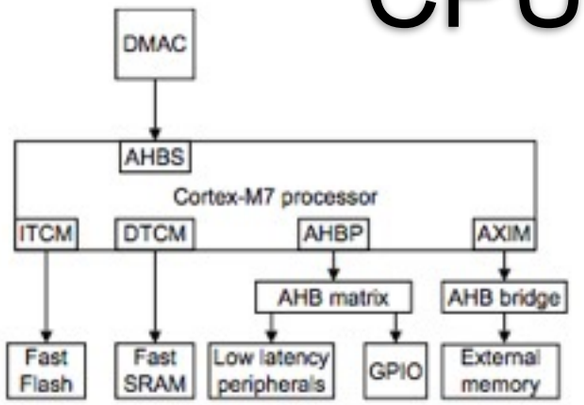


Figure 1-1 Example Cortex-M7 system

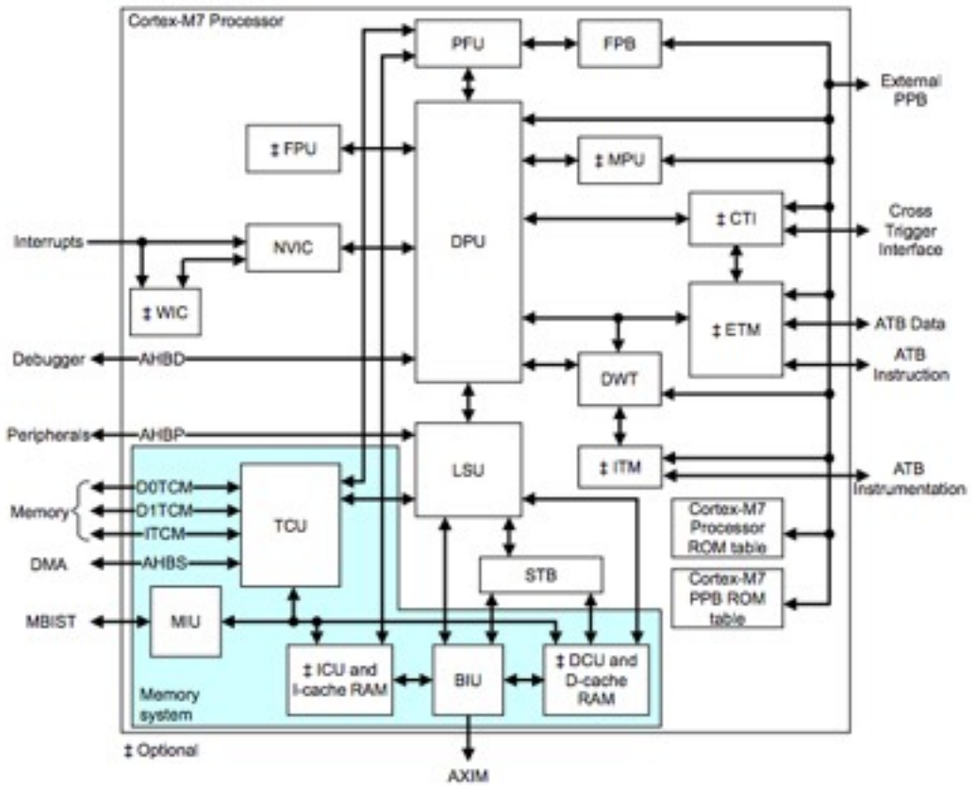
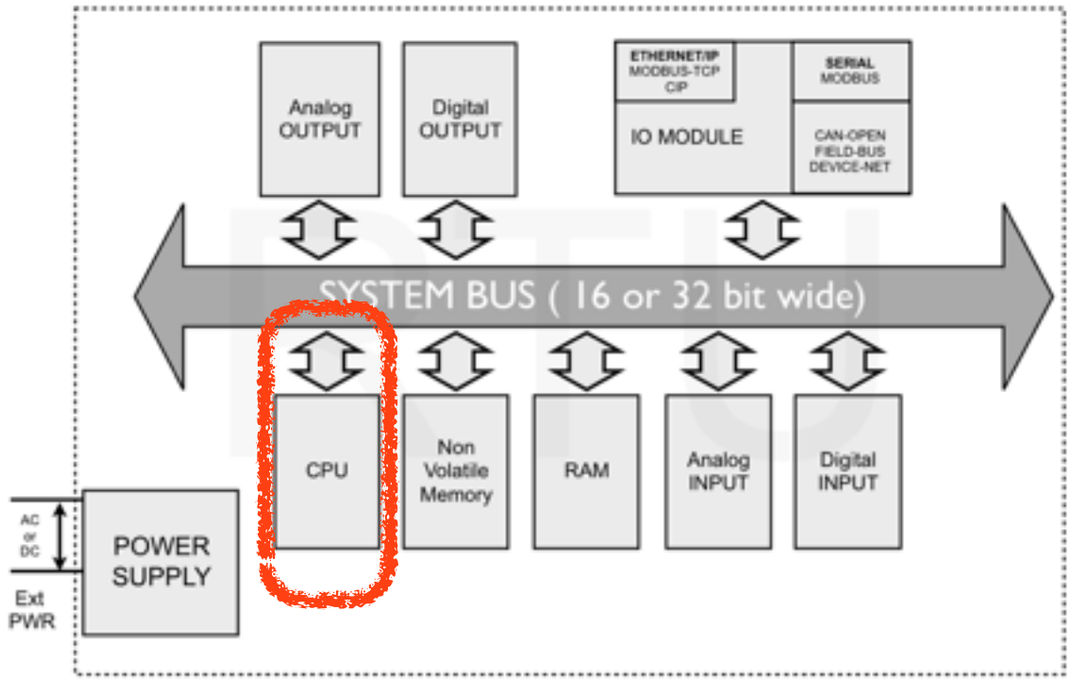


Figure 1-3 Cortex-M7 functional diagram



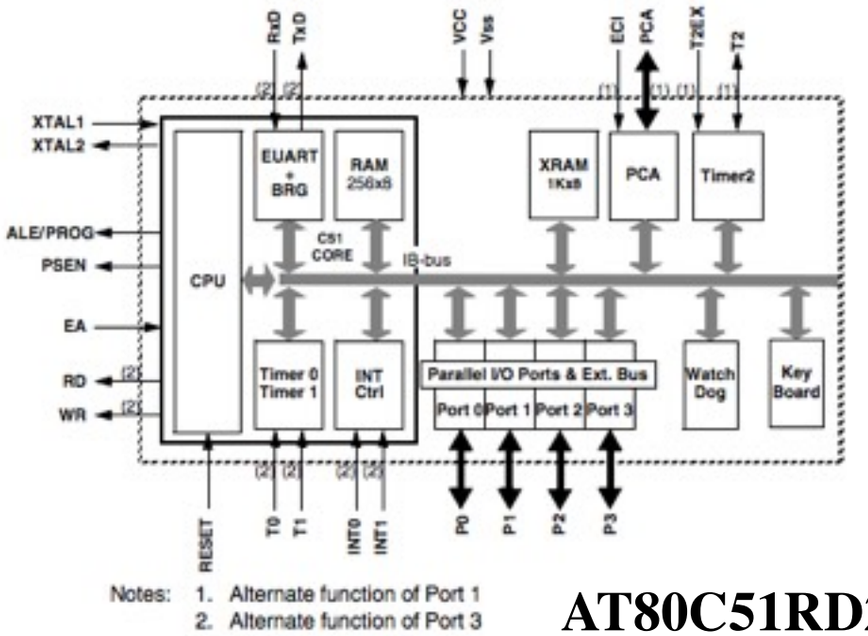
http://infocenter.arm.com/help/topic/com.arm.doc.ddi0489d/DDI0489D_cortex_m7_trm.pdf

SCADA - ARCHITECTURE

ALGONQUIN COLLEGE

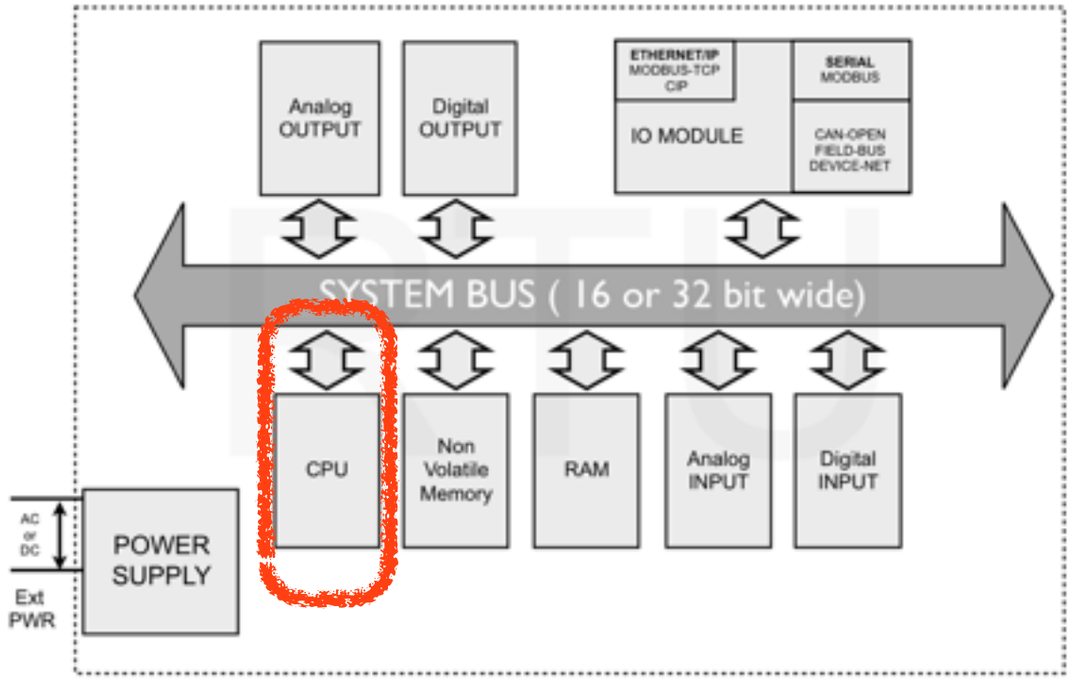
Remote Terminal Unit

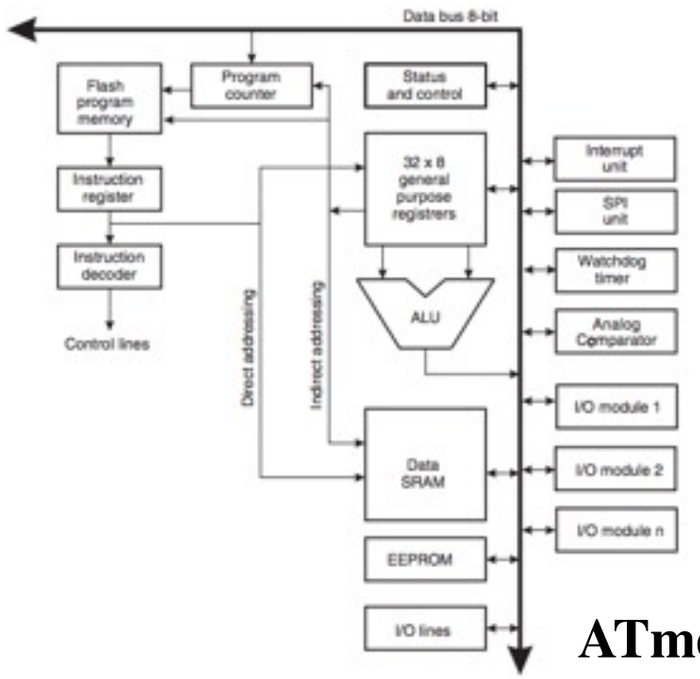
CPU



Notes: 1. Alternate function of Port 1
2. Alternate function of Port 3

AT80C51RD2





ATmega16M1

http://www.atmel.com/images/doc4113.pdf

http://www.atmel.com/images/doc8209.pdf

Remote Terminal Unit

Non Volatile Memory

Does not lose the data when power is removed

Only needs power to retrieve and save data

Relatively slow compared to Volatile RAM

EEPROM - Number of writes are limited
(around 1000 write cycles)

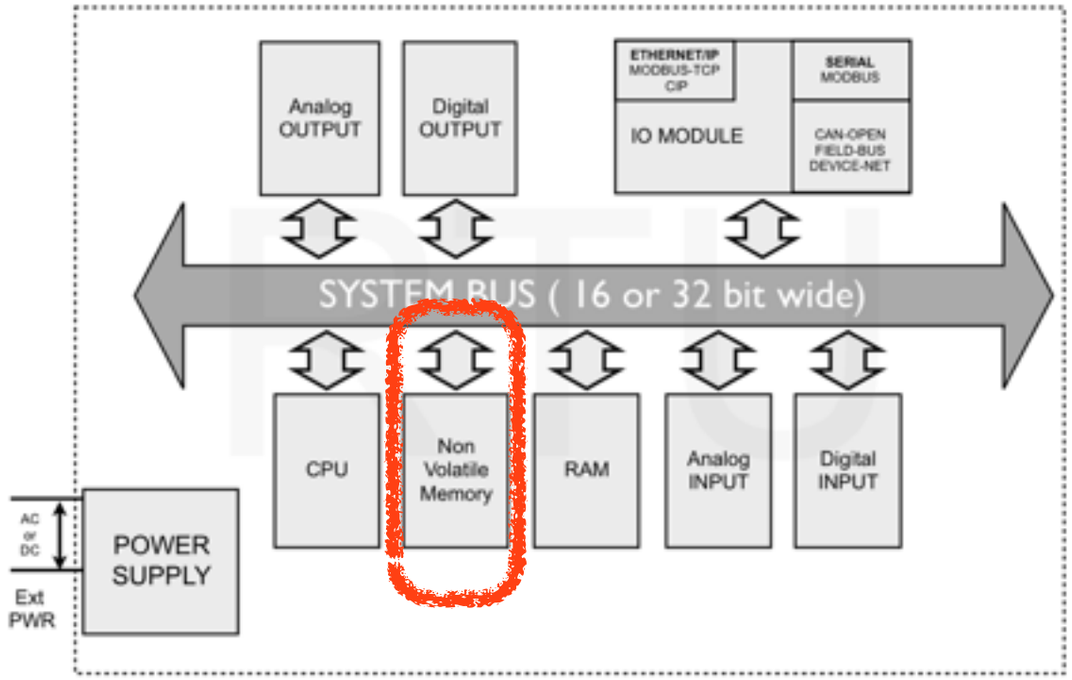
FLASH - Writes cycles also limited but much higher limit (around 10K write cycles)

Used for file system

Configuration files will be stored here

System snapshot can be stored at regular intervals

USB Memory stick is an example of FLASH memory



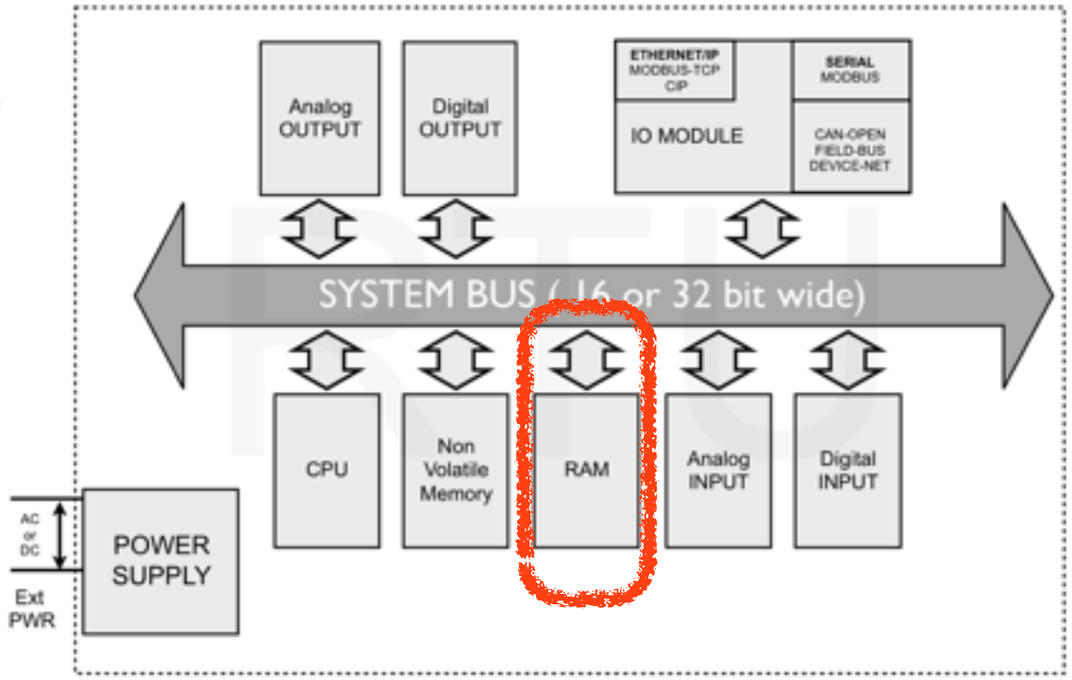
http://www.zetta.net/history-of-computer-storage/

https://en.wikipedia.org/wiki/Computer_memory

https://en.wikipedia.org/wiki/Non-volatile_memory

Remote Terminal Unit

Random **A**ccess **M**emory



Two main types - DRAM and SRAM

Needs to be refreshed constantly

Faster then FLASH memory for now

http://www.zetta.net/history-of-computer-storage/

https://en.wikipedia.org/wiki/Computer_memory

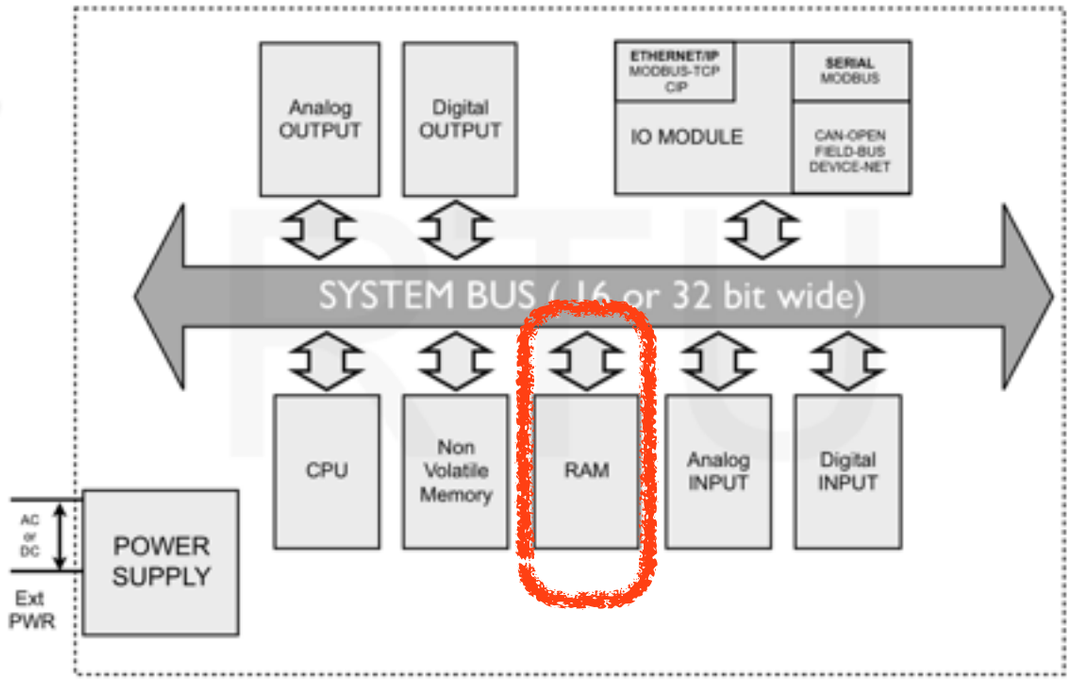
https://en.wikipedia.org/wiki/Random-access_memory

https://www.youtube.com/watch?v=P12r8DKHsak

https://www.youtube.com/watch?v=YIBhPsyYCiM

Remote Terminal Unit

Random **A**ccess **M**emory



Where the CPU reads the current runtime software

The status of the inputs is stored in RAM

Results of measurements are stored in RAM as a buffer for transmission to the SCADA master

In RTU memory is organized around the communications protocols the RTU supports

Remote Terminal Unit

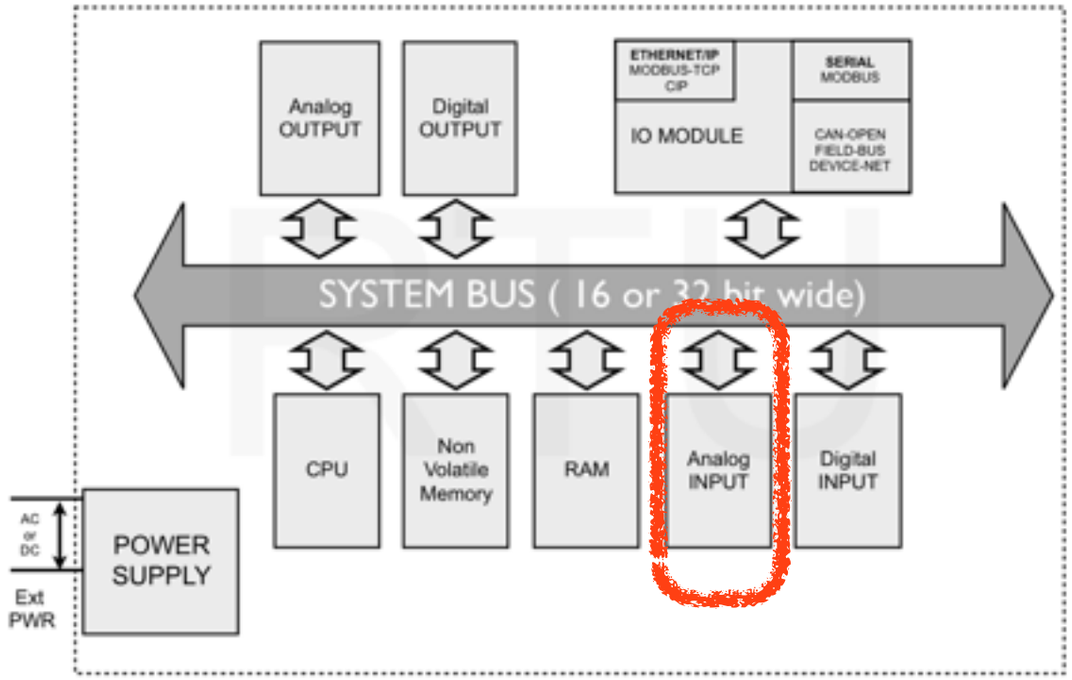
Analog - INPUT

Any analog input has to be digitized

ADC resolution is usually between 12 - 16 bits

INT vs FLOAT

IEEE 754 - Standard for Floating Numbers



https://en.wikipedia.org/wiki/Analog-to-digital_converter

https://en.wikipedia.org/wiki/Sensor

SCADA - ARCHITECTURE

ALGONQUIN COLLEGE

Remote Terminal Unit

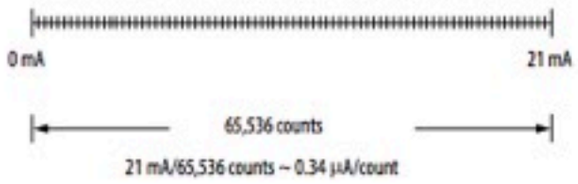
Module Resolution

Resolution is the smallest amount of change that the module can detect. Analog input modules are capable of 16-bit resolution. Output modules are capable of 13...16 bit resolution, depending on the module type.

The 16 bits represent 65,536 counts. This total is fixed but the value of each count is determined by the operational range you choose for your module.

For example, if you are using the 1756-IF6I module, your module's available current range equals 21 mA. Divide your range by the number of counts to figure out the value of each count. In this case, one count is approximately 0.34 µA.

Figure 2 - Module Resolution



IMPORTANT A module's resolution is fixed. It does not change regardless of what data format you choose or how you decide to scale your module in floating point mode.

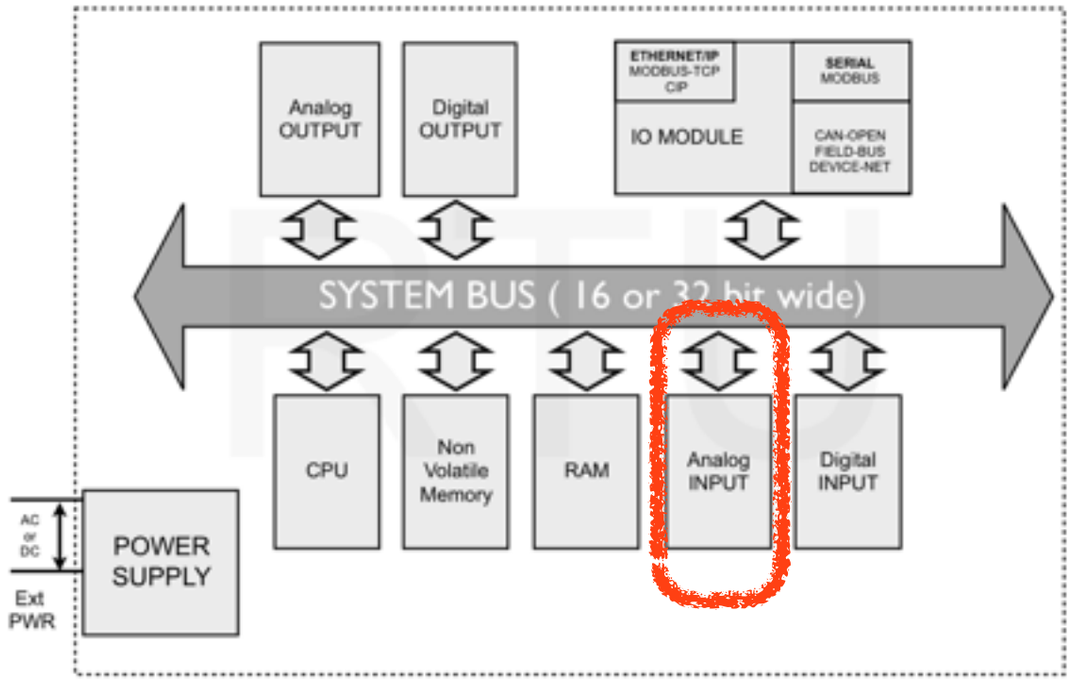
Resolution is based on the module hardware and the range selected. If you use a sensor with limited range, you do not change the module resolution.

The table lists the resolution for each module's range.

Table 3 - Current Values Represented in Engineering Units

Module	Range	Number of significant bits	Resolution
1756-IF16 and 1756-IF8	+/- 10.25V 0...10.25V 0...5.125V 0...20.5 mA	16 bits	320 µV/count 160 µV/count 80 µV/count 0.32 µA/count
1756-IF6CIS	0 mA...21 mA	16 bits	0.34 µA/count
1756-IF6I	+/- 10.5V 0...10.5V 0...5.25V 0...21 mA	16 bits	343 µV/count 171 µV/count 86 µV/count 0.34 µA/count

Rockwell Automation Publication 1756-UM009D-EN-P - March 2015



Analog - INPUT

SCADA - ARCHITECTURE

ALGONQUIN COLLEGE

Remote Terminal Unit

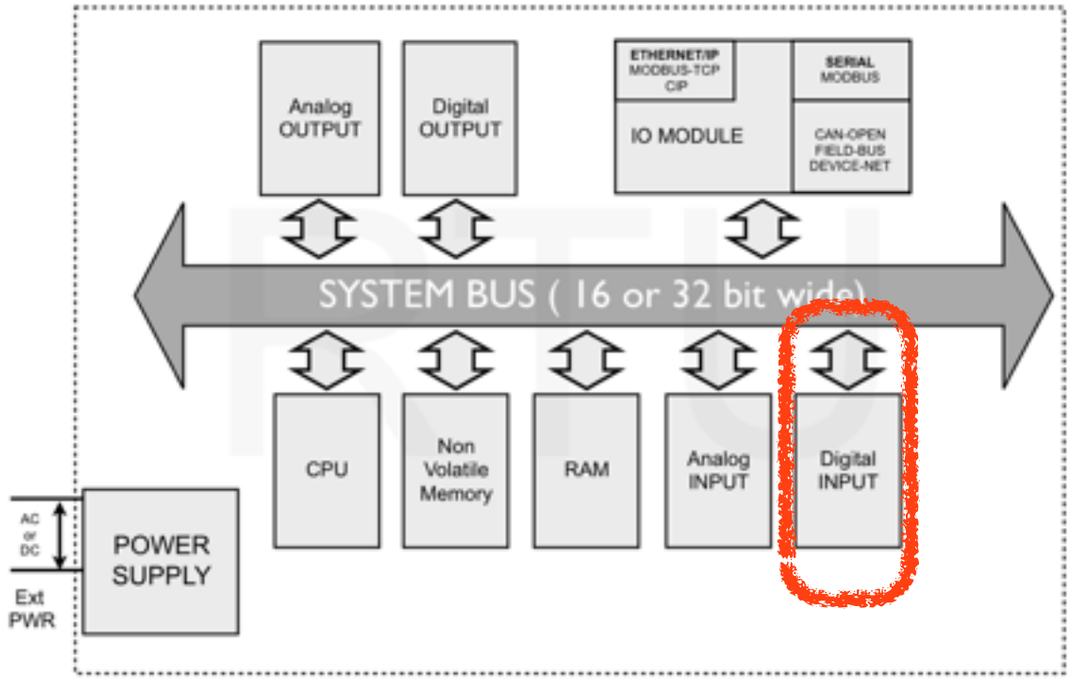
Digital - INPUT

Contains protection from voltage spikes

Uses opto-isolators to electrically isolate the input from the internal circuitry

Looks for ON / OFF conditions

Reads relays or switches



Remote Terminal Unit

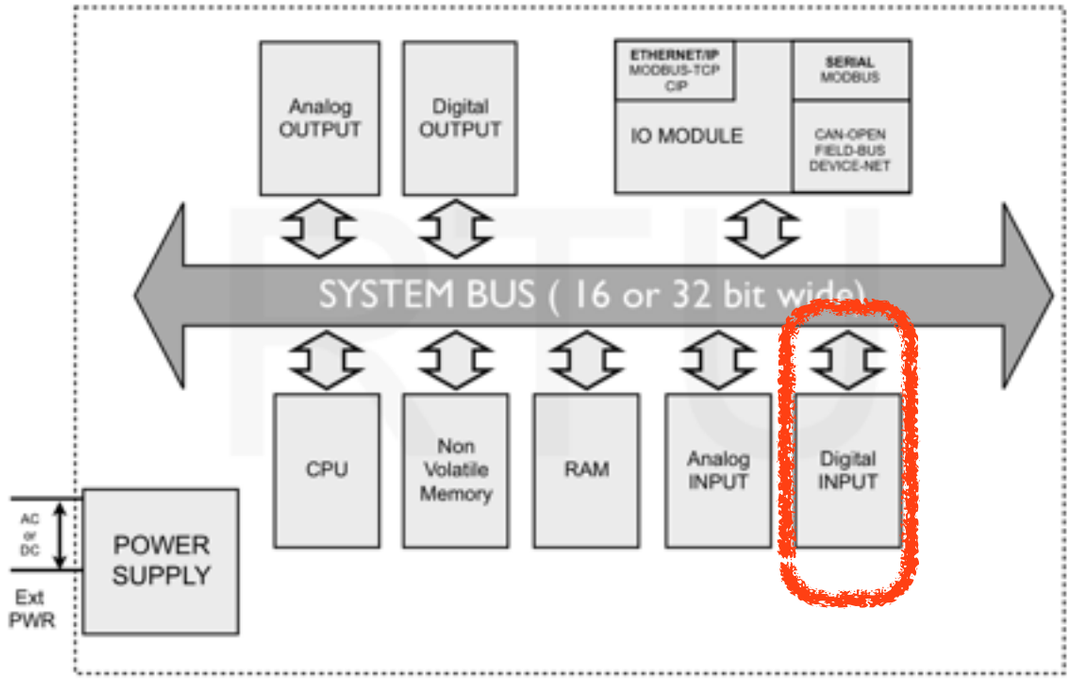
Digital - INPUT

Contains protection from voltage spikes

Uses opto-isolators to electrically isolate the input from the internal circuitry

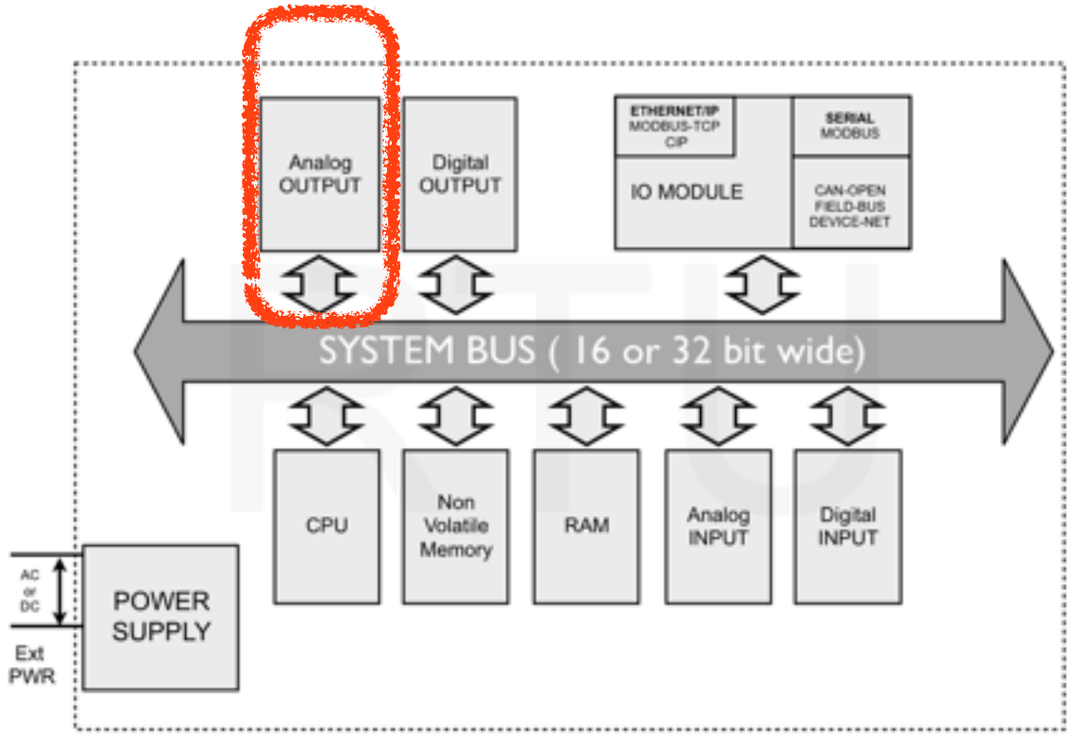
Looks for ON / OFF conditions

Reads relays or switches



Remote Terminal Unit

Analog - OUTPUT



Control a voltage or current source

Current and voltage sources are derived from a D/A (Digital to Analog) converter

12 - 16 bit resolution

PWM

https://en.wikipedia.org/wiki/Digital-to-analog_converter

https://en.wikipedia.org/wiki/Current_loop

https://en.wikipedia.org/wiki/Transimpedance_amplifier

https://en.wikipedia.org/wiki/Pulse-width_modulation

Remote Terminal Unit

Digital - OUTPUT

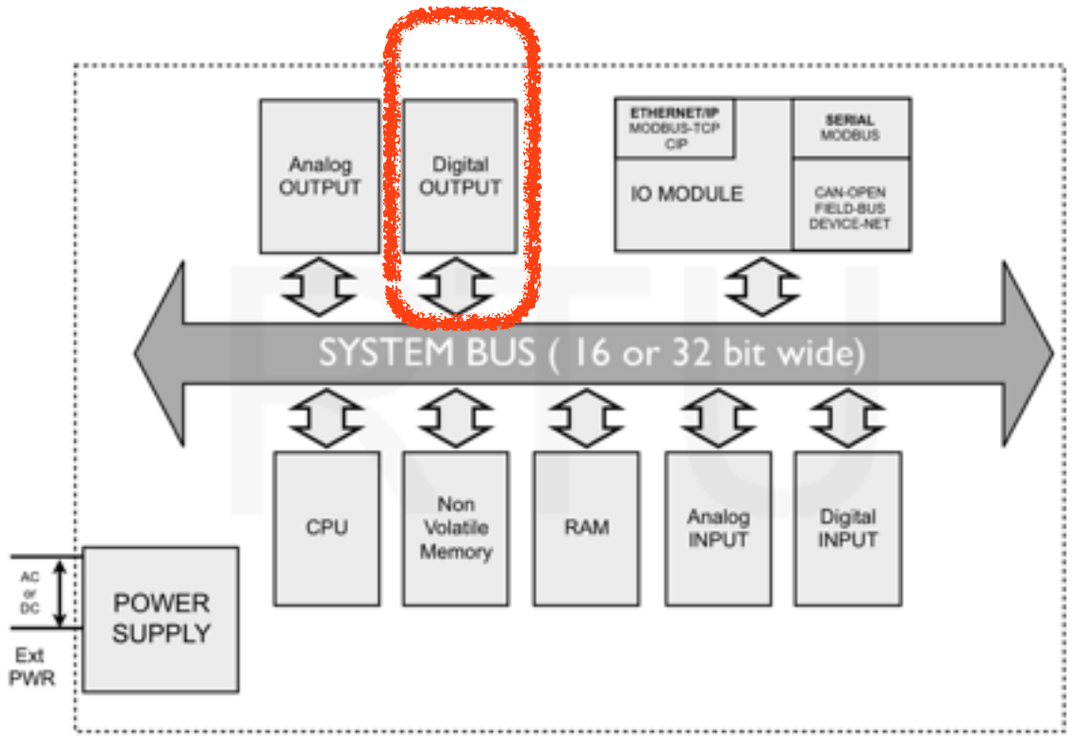
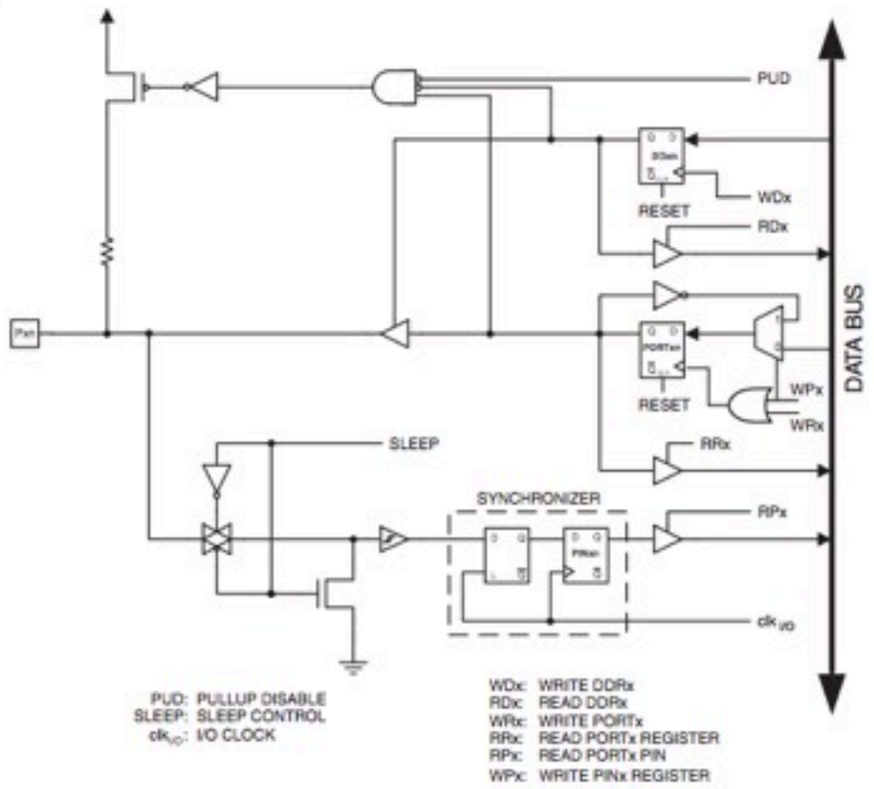


Figure 13-2. General digital I/O [1].



Note: 1. WRx, WPx, WDx, RRx, RPx, and RDx are common to all pins within the same port. $clk_{I/O}$, SLEEP, and PUD are common to all ports.

Configuring the pin

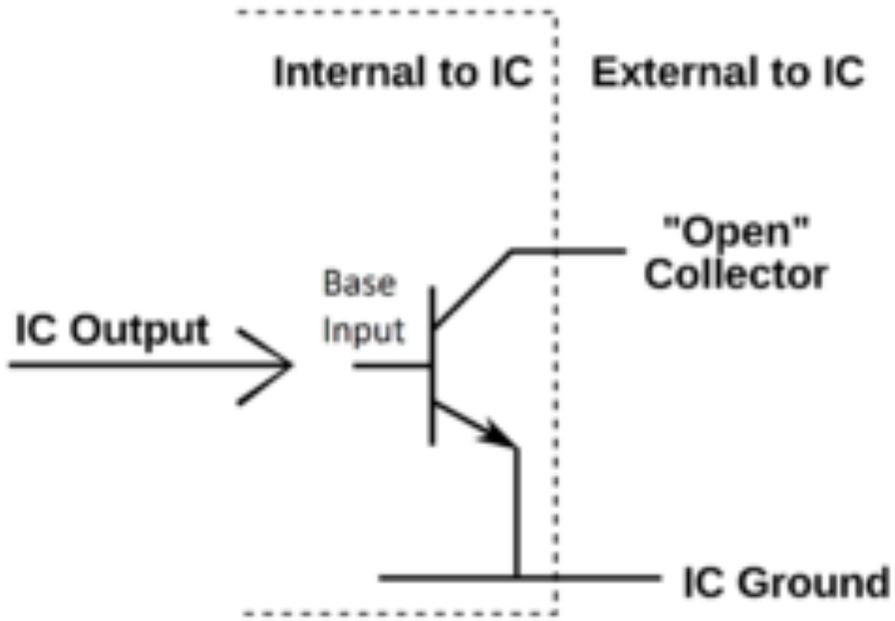
Each port pin consists of three register bits: DDxn, PORTxn, and PINxn. As shown in "Register description" on page 78, the DDxn bits are accessed at the DDRx I/O address, the PORTxn bits at the PORTx I/O address, and the PINxn bits at the PINx I/O address.

The DDxn bit in the DDRx Register selects the direction of this pin. If DDxn is written logic one, Pxn is configured as an output pin. If DDxn is written logic zero, Pxn is configured as an input pin.

If PORTxn is written logic one when the pin is configured as an input pin, the pull-up resistor is activated. To switch the pull-up resistor off, PORTxn has to be written logic zero or the pin has to be configured as an output pin.

The port pins are tri-stated when reset condition becomes active, even if no clocks are running.

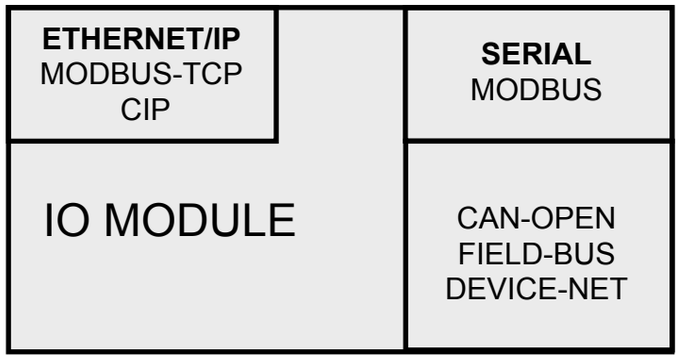
If PORTxn is written logic one when the pin is configured as an output pin, the port pin is driven high (one). If PORTxn is written logic zero when the pin is configured as an output pin, the port pin is driven low (zero).

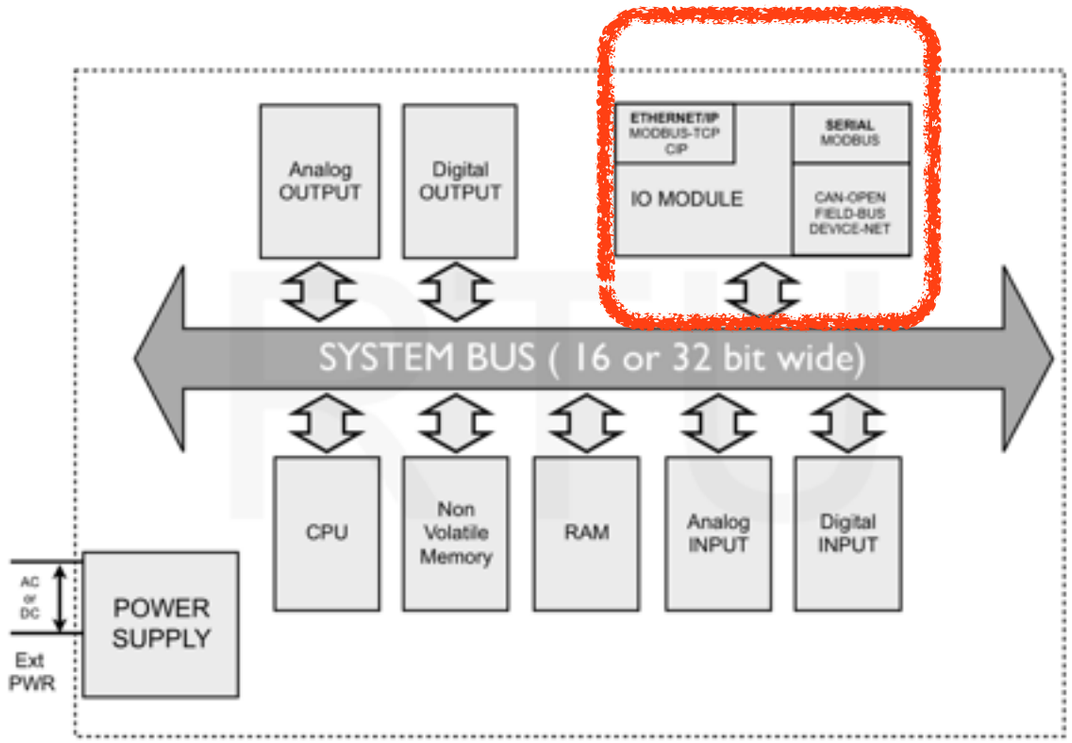


SCADA - ARCHITECTURE

Remote Terminal Unit

I/O Module





Provides all communications to the outside world

Usually supports several communications protocols

Must decode/encode each protocol from the data-bus

Older units have low bandwidth

Really old units might have only serial ports that run at 9600 Baud

PWM

https://en.wikipedia.org/wiki/Input/output

https://en.wikipedia.org/wiki/Modbus

https://en.wikipedia.org/wiki/EtherNet/IP

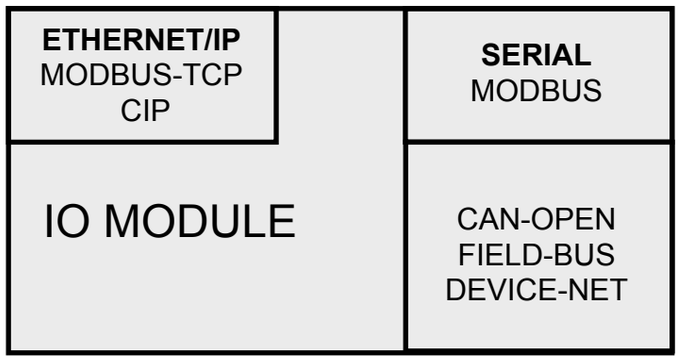
https://en.wikipedia.org/wiki/CANopen

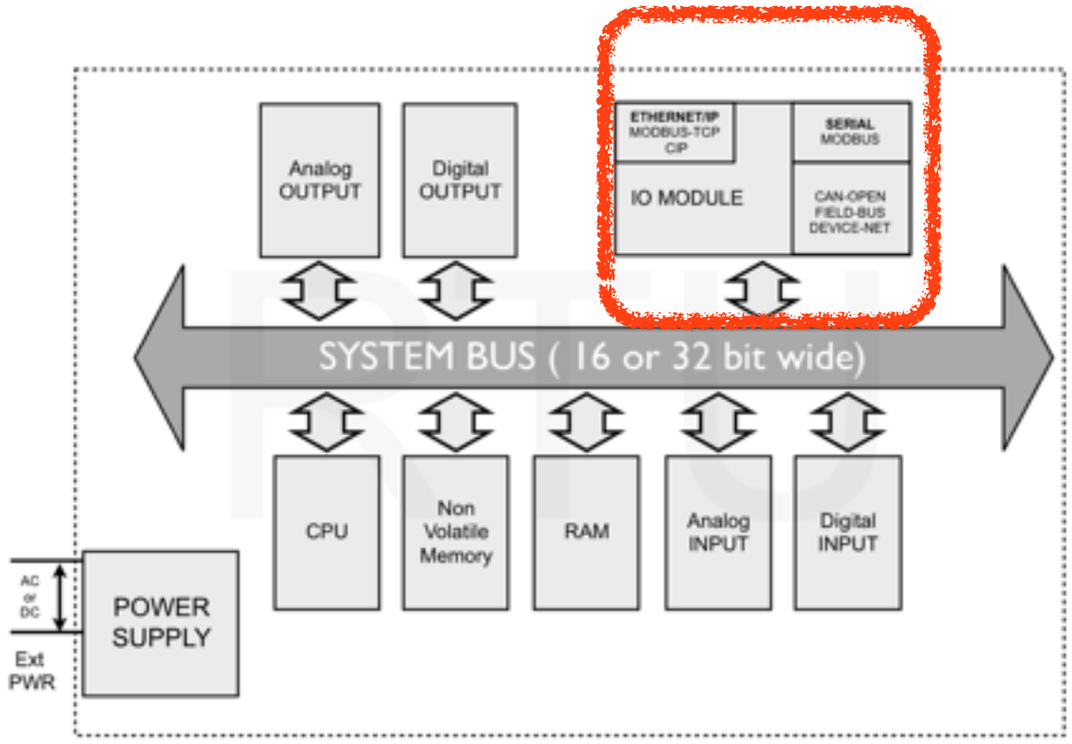
SCADA - ARCHITECTURE

ALGONQUIN COLLEGE

Remote Terminal Unit

I/O Module





MODBUS RTU

ETHERNET/IP

MODBUS TCP

FIELD BUS

CANopen

https://en.wikipedia.org/wiki/Input/output

https://en.wikipedia.org/wiki/Modbus

https://en.wikipedia.org/wiki/EtherNet/IP

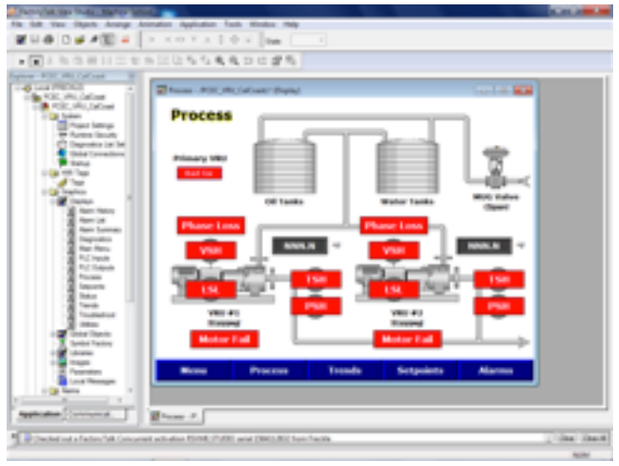
https://en.wikipedia.org/wiki/CANopen

https://en.wikipedia.org/wiki/Fieldbus

SYSTEM ARCHITECTURE

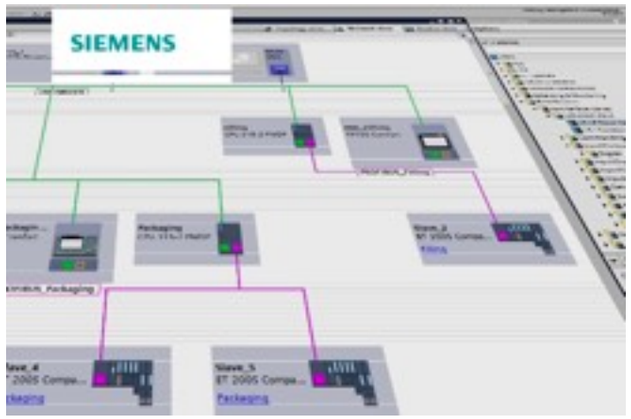
Master Controller

Master Controller

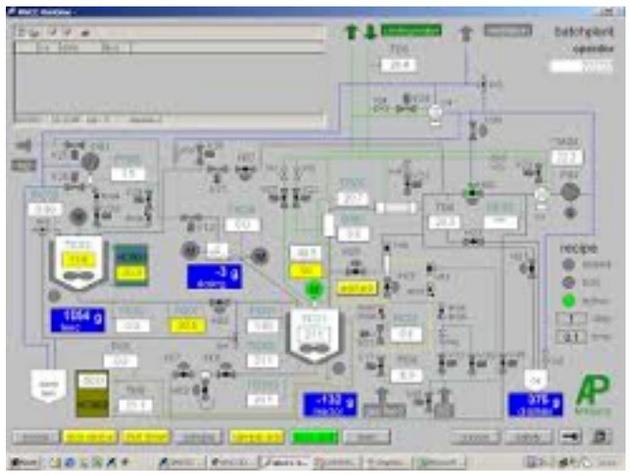


Factory Talk (Rockwell)

OEM Windows Server

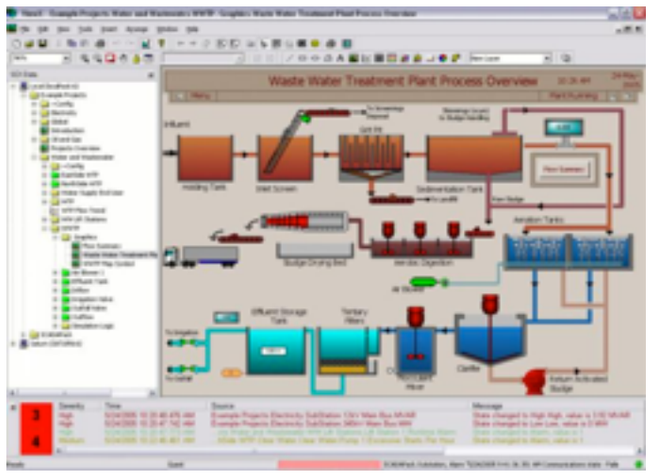


SIMATIC (Siemens)



WinCC (Siemens)

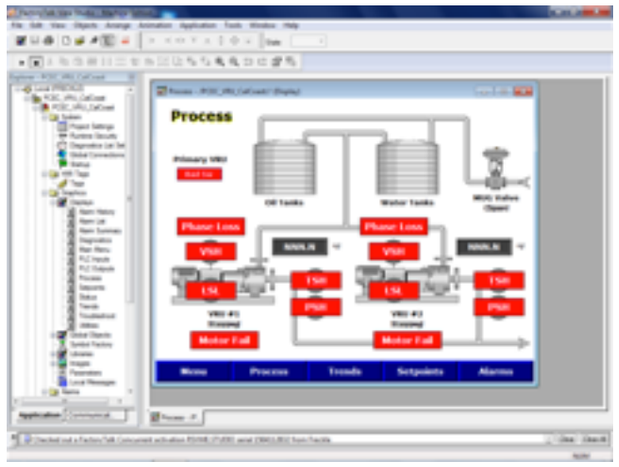
ClearSCADA (Schneider)



SCADA - ARCHITECTURE

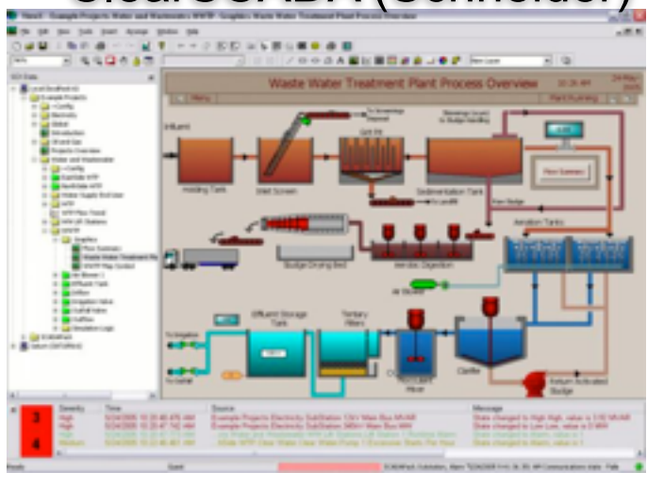
ALGONQUIN COLLEGE

Master Controller



Factory Talk (Rockwell)

ClearSCADA (Schneider)



We have access to Factory Talk ME and SE versions

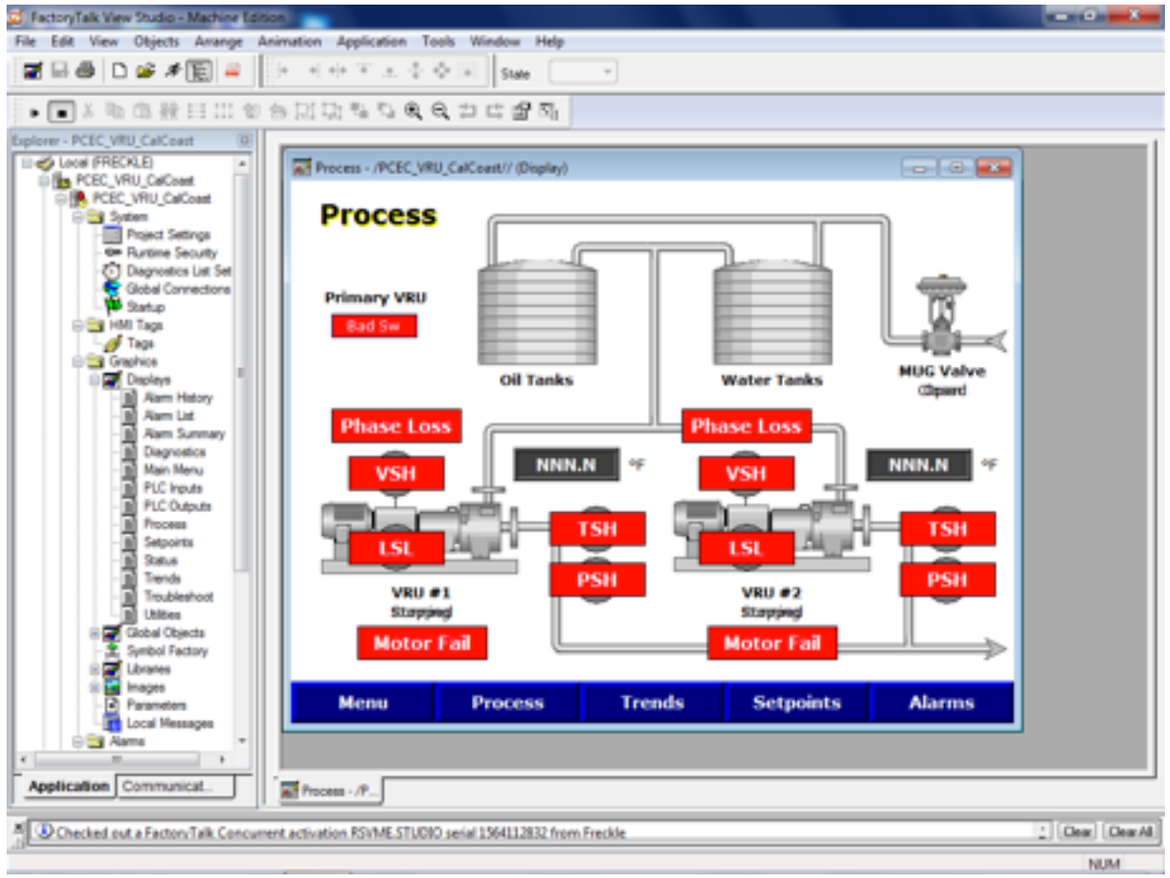
ClearSCADA is available as a demo

SCADA - ARCHITECTURE

ALGONQUIN COLLEGE

Master Controller

Factory Talk (Rockwell)



Provides everything needed to develop a full SCADA application

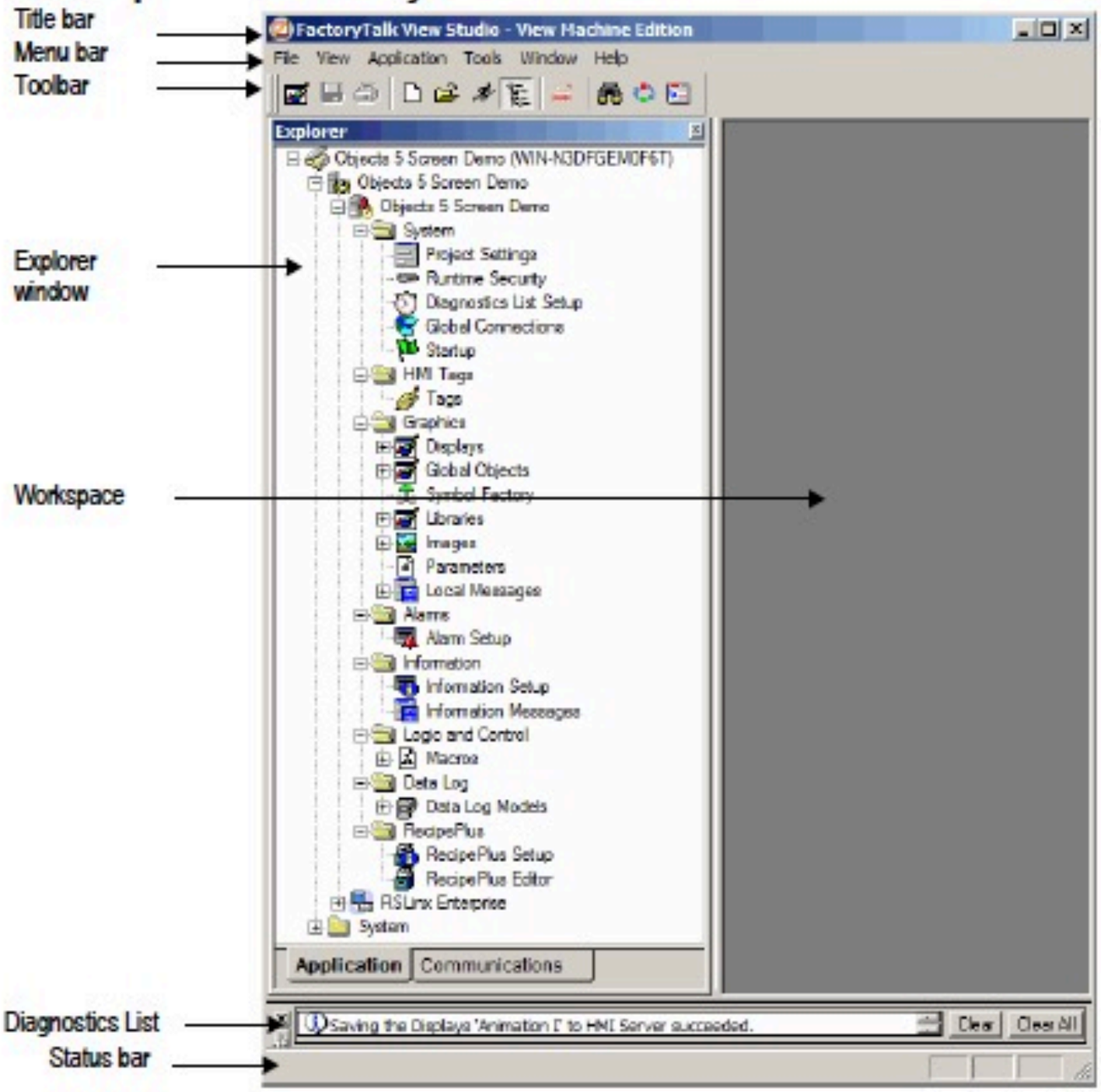
Entire project is shown in a graphical form

Very similar to IDE for writing software

SCADA - ARCHITECTURE

ALGONQUIN COLLEGE

Master Controller



Shows entire project at once

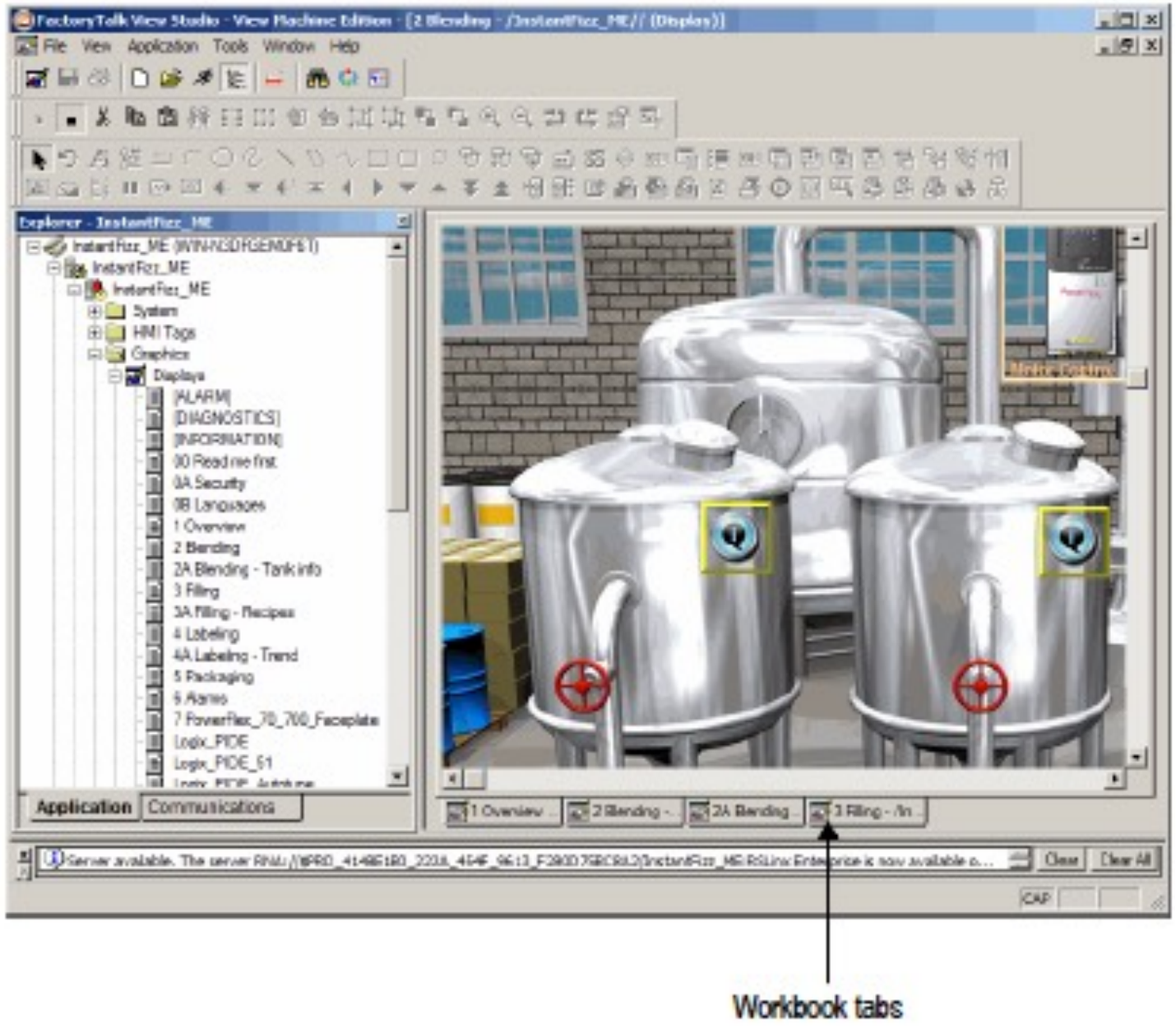
Each aspect of the program is a folder in the file tree

In Computer Science this is called an Integrated Development Environment

SCADA - ARCHITECTURE

ALGONQUIN COLLEGE

Master Controller



Develop HMI screens for systems operators

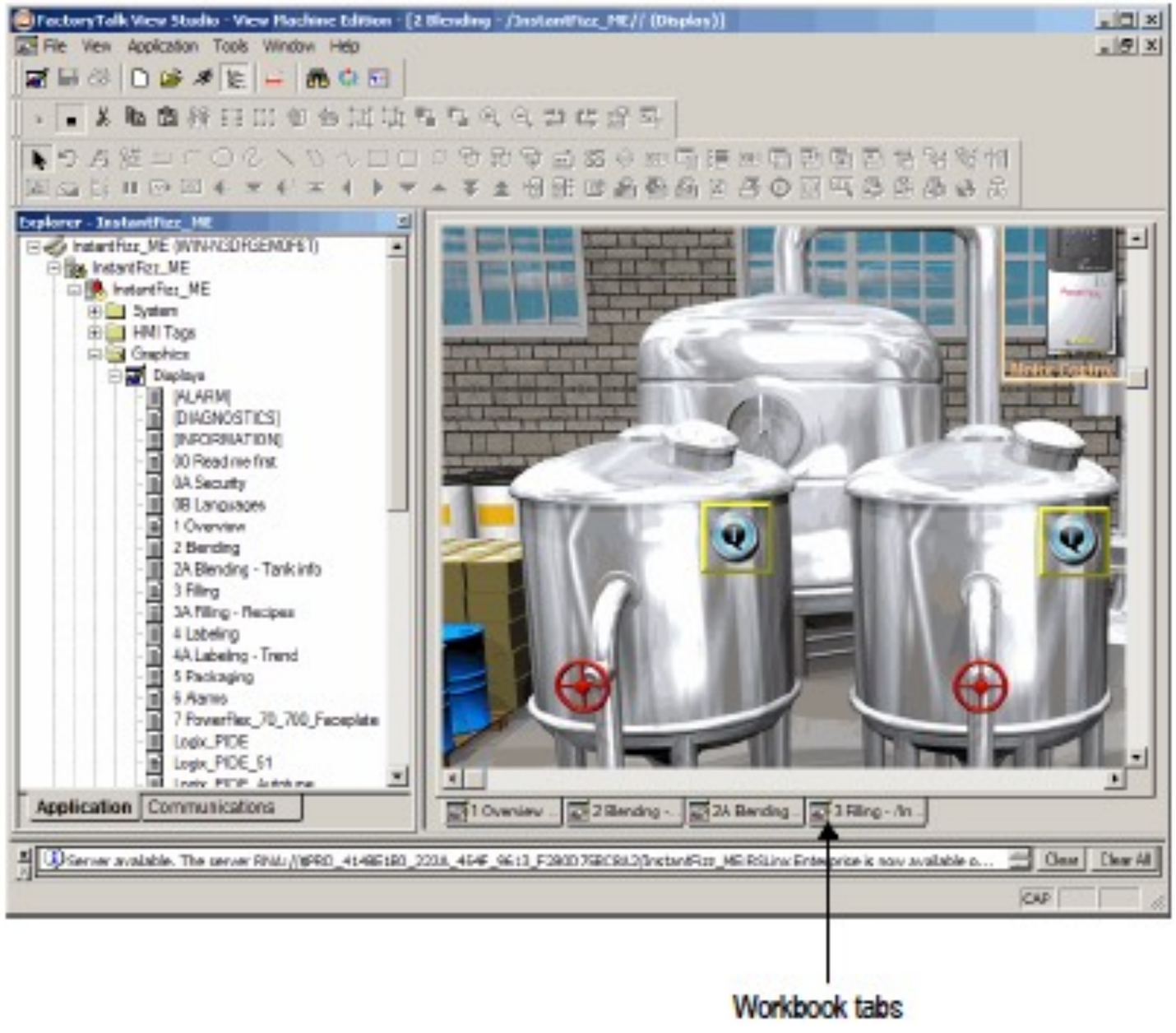
PLC tags and Alarms

Setup a database (Historian) to capture alarms and events through the tags

SCADA - ARCHITECTURE

ALGONQUIN COLLEGE

Master Controller



Develop HMI screens for systems operators

PLC tags and Alarms

Setup a database (Historian) to capture alarms and events through the tags

SCADA - ARCHITECTURE

ALGONQUIN COLLEGE

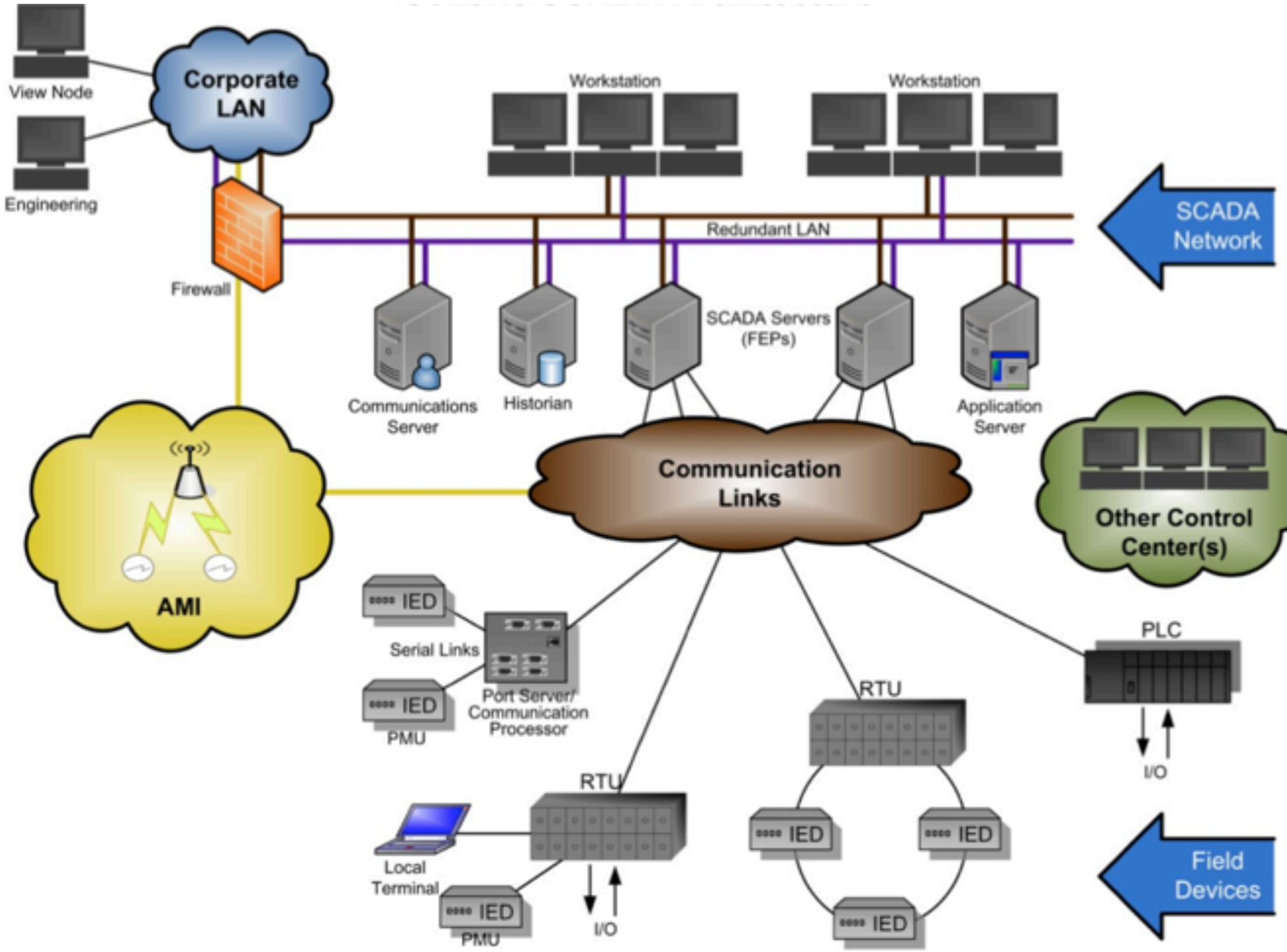
SYSTEM ARCHITECTURE

Communications

SCADA - ARCHITECTURE

ALGONQUIN COLLEGE

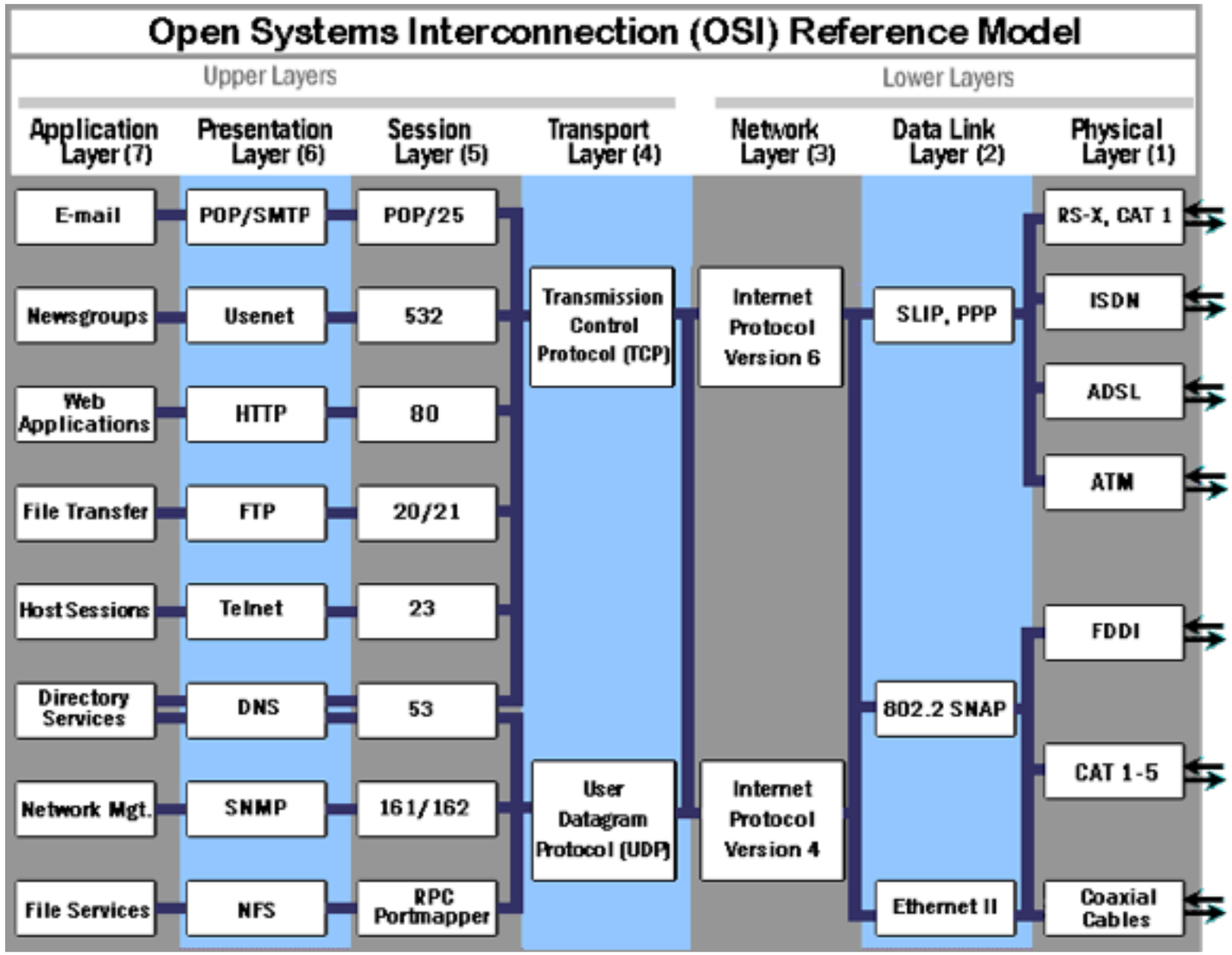
Communications

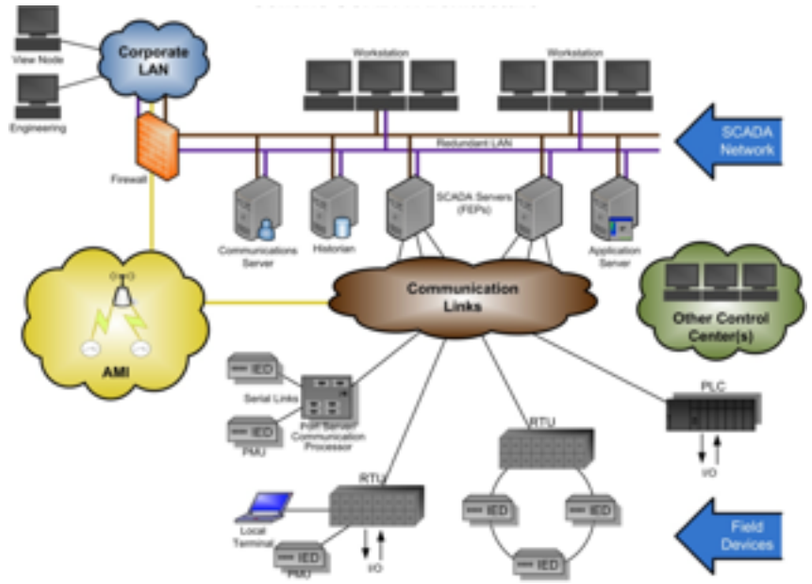


SCADA - ARCHITECTURE

ALGONQUIN COLLEGE

Communications





OSI abstracts the network elements

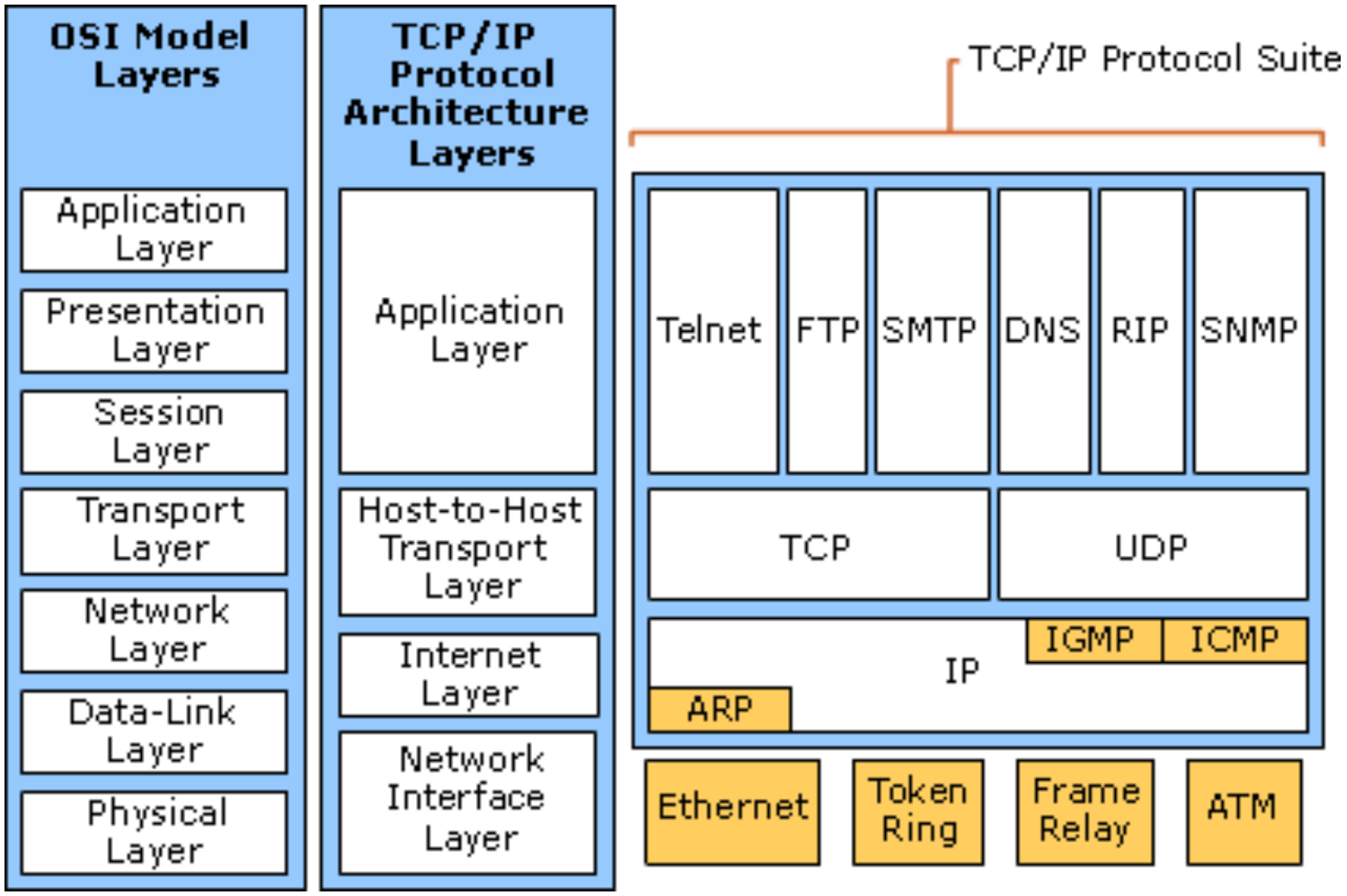
Allows many vendors to compete in each “Layer”

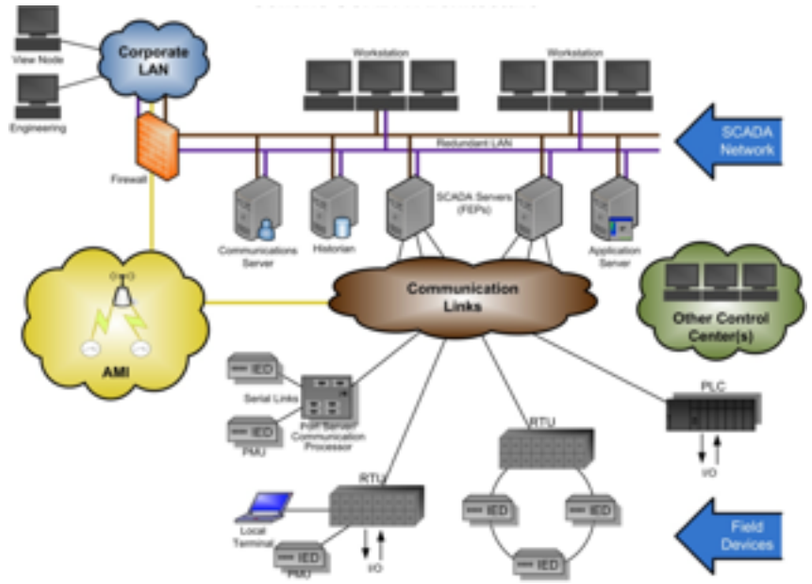
Protocols fit into the model

SCADA - ARCHITECTURE

ALGONQUIN COLLEGE

Communications





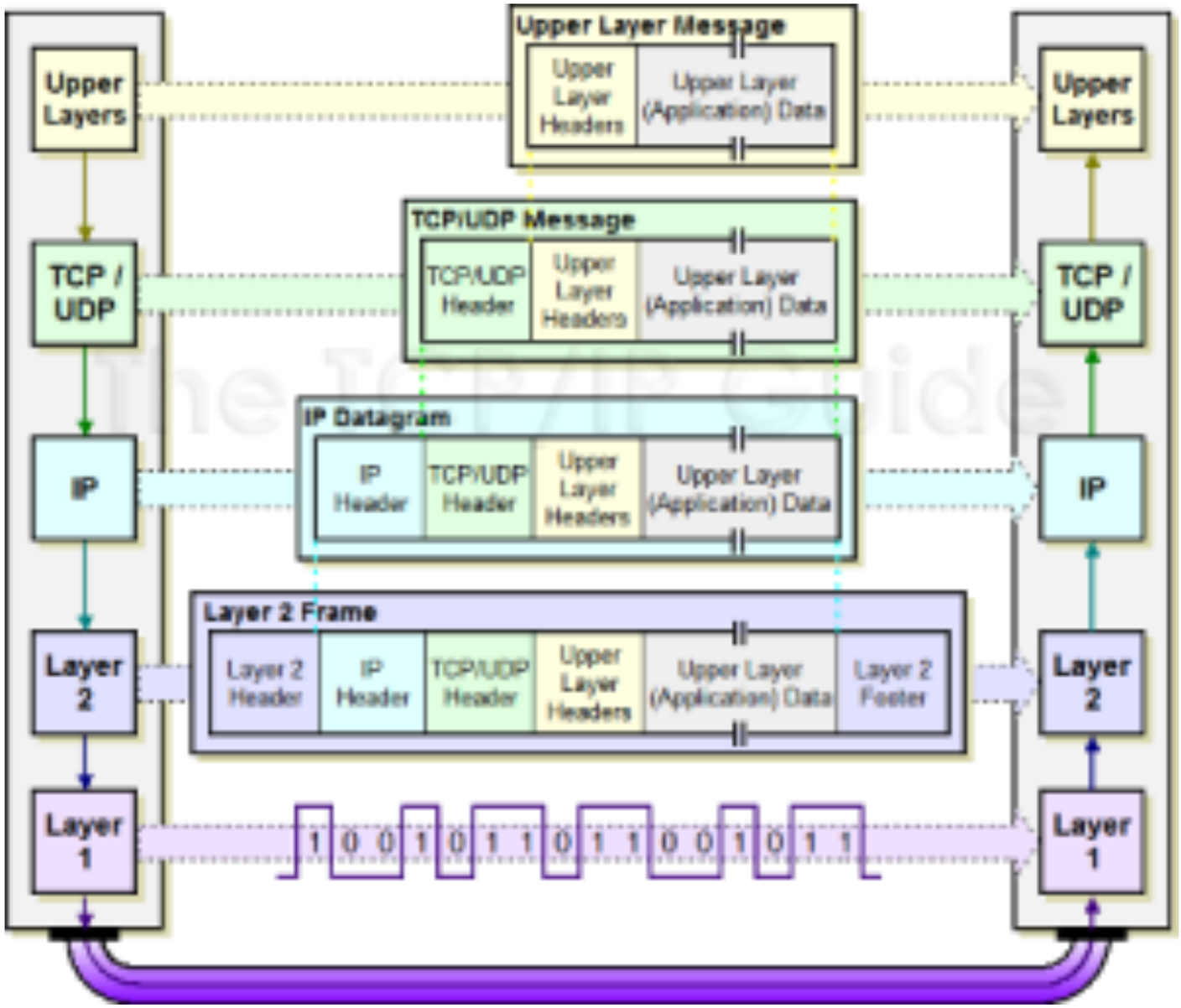
TCP/IP maps four layers to the OSI seven layer model

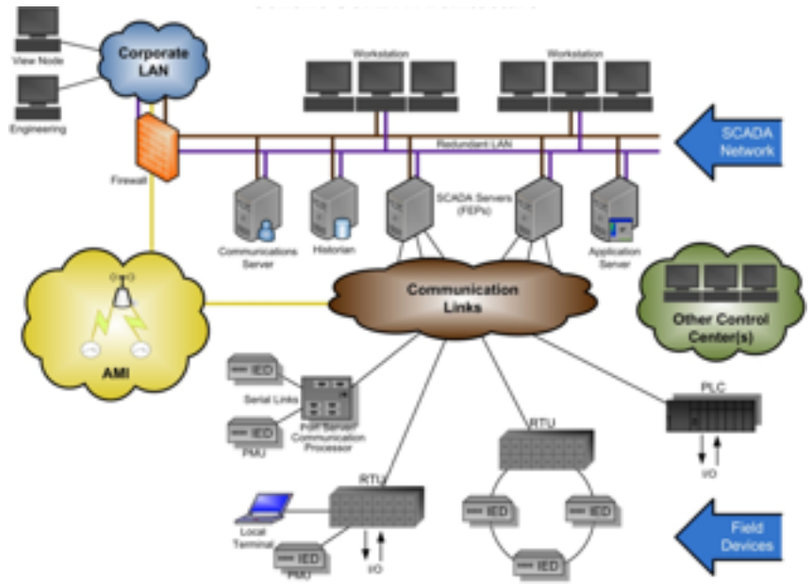
TCP/IP over Ethernet is becoming the standard for everything connected

SCADA - ARCHITECTURE

ALGONQUIN COLLEGE

Communications





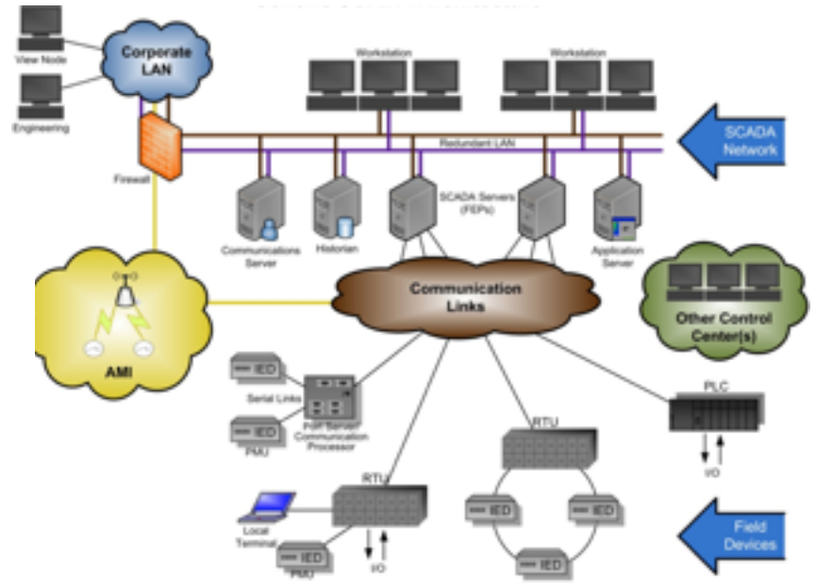
SCADA - ARCHITECTURE

ALGONQUIN COLLEGE

Communications

OSI (Open Source Interconnection) 7 Layer Model

Layer	Application/Example		Central Device/ Protocols		DOD4 Model
Application (7) Serves as the window for users and application processes to access the network services.	**End User layer** Program that opens what was sent or creates what is to be sent Resource sharing • Remote file access • Remote printer access • Directory services • Network management		**User Applications** SMTP	GATEWAY Can be used on all layers	Process
Presentation (6) Formats the data to be presented to the Application layer. It can be viewed as the "Translator" for the network.	**Syntax layer** encrypt & decrypt (if needed) Character code translation • Data conversion • Data compression • Data encryption • **Character Set Translation**		JPEG/ASCII EBDIC/TIFF/GIF PICT		
Session (5) Allows session establishment between processes running on different stations.	**Synch & send to ports** (logical ports) Session establishment, maintenance and termination • Session support - perform security, name recognition, logging, etc.		**Logical Ports** RPC/SQL/NFS NetBIOS names		
Transport (4) Ensures that messages are delivered error-free, in sequence, and with no losses or duplications.	**TCP** Host to Host, Flow Control Message segmentation • Message acknowledgement • Message traffic control • Session multiplexing	PACKET FILTERING	TCP/SPX/UDP		Host to Host
Network (3) Controls the operations of the subnet, deciding which physical path the data takes.	**Packets** ("letter", contains IP address) Routing • Subnet traffic control • Frame fragmentation • Logical-physical address mapping • Subnet usage accounting		**Routers** IP/IPX/ICMP		Internet
Data Link (2) Provides error-free transfer of data frames from one node to another over the Physical layer.	**Frames** ("envelopes", contains MAC address) [NIC card — Switch — NIC card] (end to end) Establishes & terminates the logical link between nodes • Frame traffic control • Frame sequencing • Frame acknowledgment • Frame delimiting • Frame error checking • Media access control		**Switch Bridge WAP** PPP/SLIP	Land Based Layers	Network
Physical (1) Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.	**Physical structure** Cables, hubs, etc. Data Encoding • Physical medium attachment • Transmission technique - Baseband or Broadband • Physical medium transmission Bits & Volts		**Hub**		



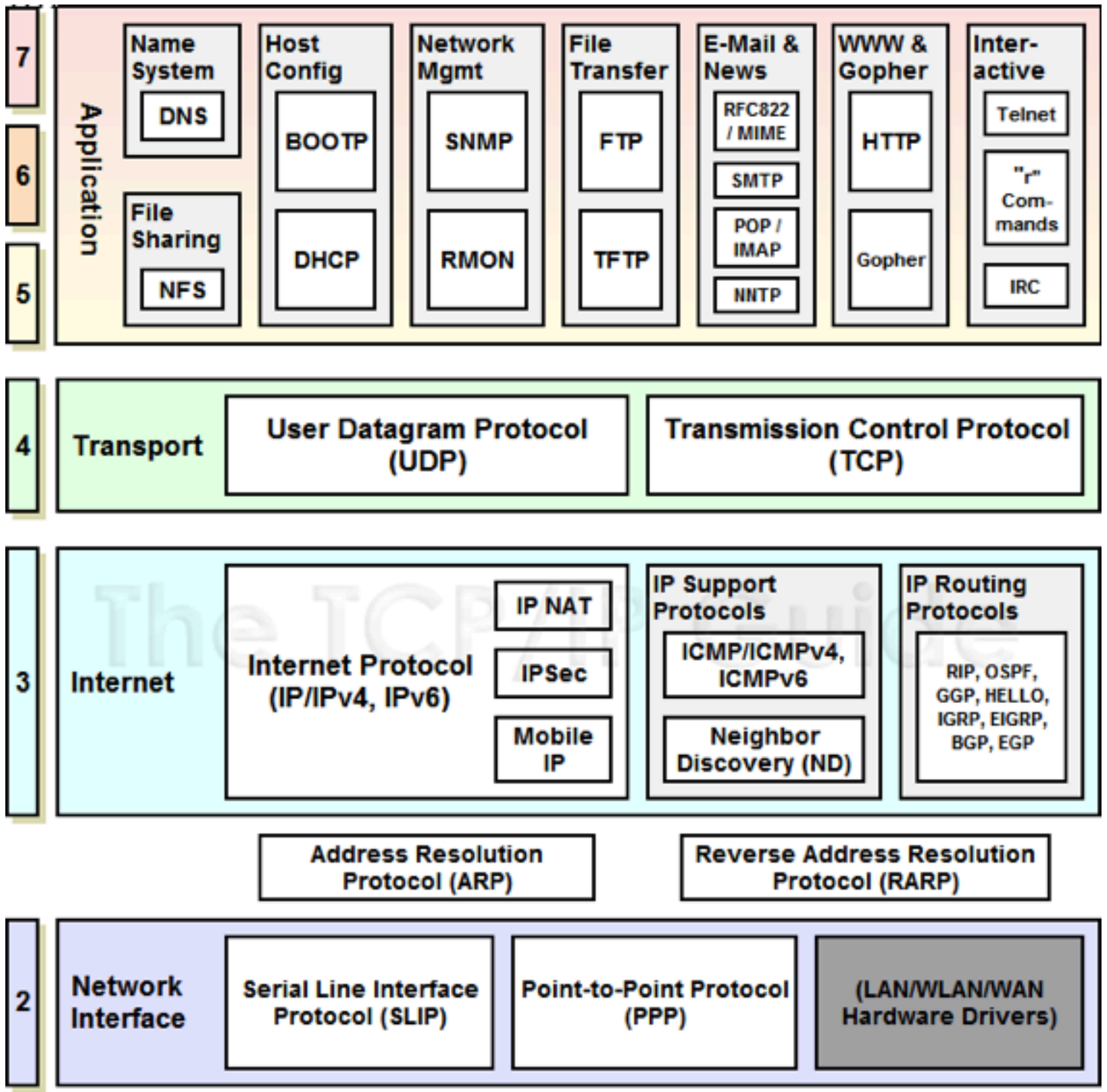
TCP/IP maps four layers to the OSI seven layer model

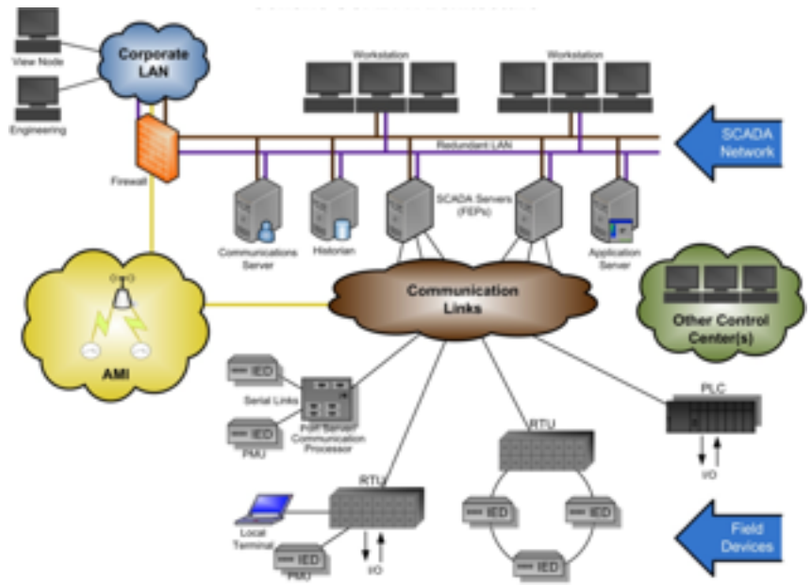
TCP/IP over Ethernet is becoming the standard for everything connected

SCADA - ARCHITECTURE

ALGONQUIN COLLEGE

Communications





Network protocols mapped to the different layers

Confusion in numbering layers

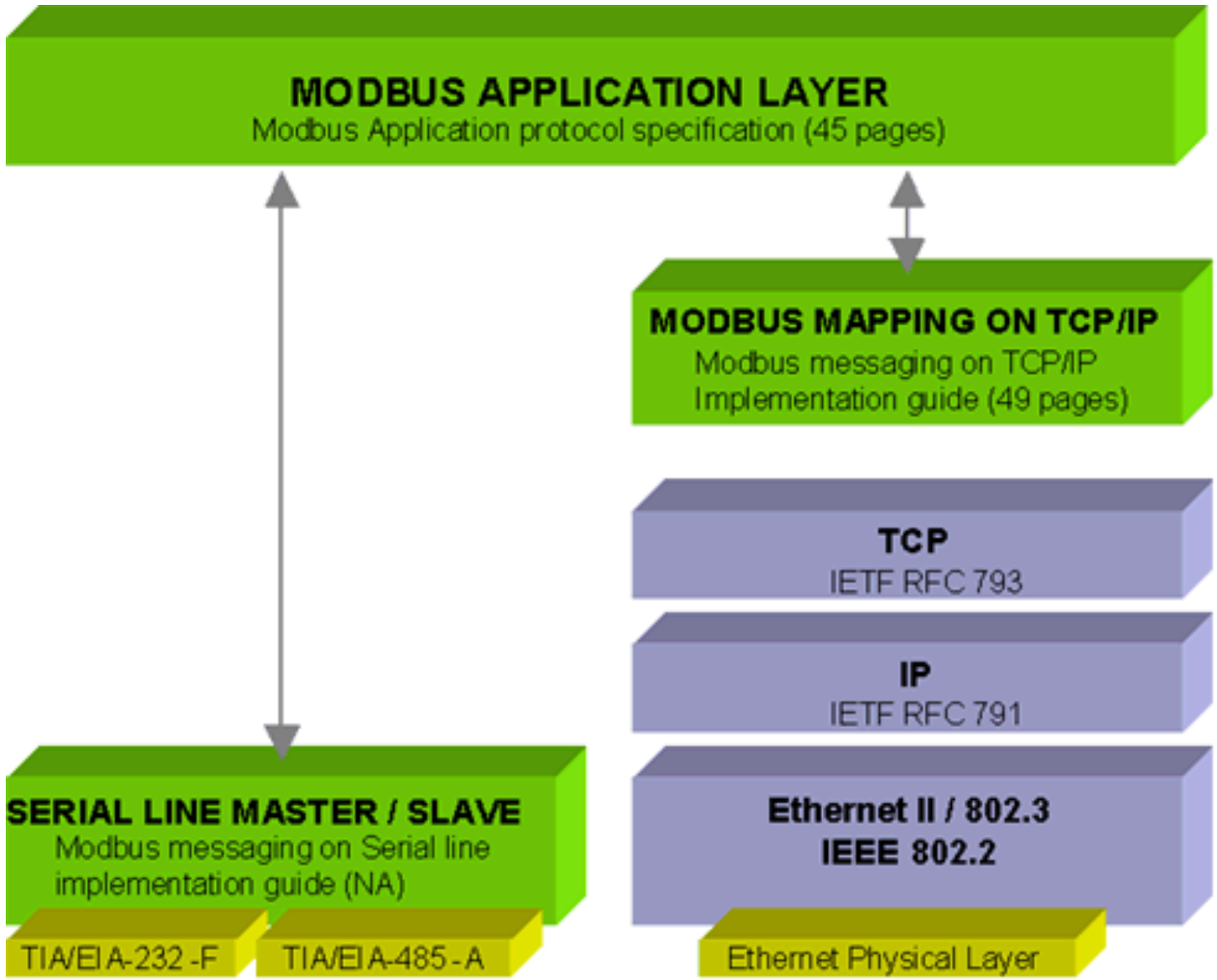
Network architecture involves designing network at each layer

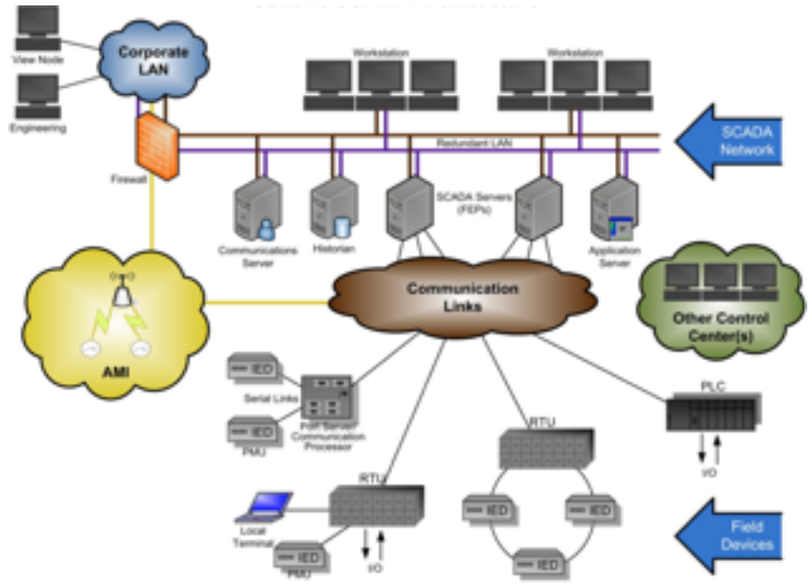
Usually takes a top down approach

SCADA - ARCHITECTURE

ALGONQUIN COLLEGE

Communications





MODBUS-RTU
Maps to Layer 1,2, and 7 of OSI

RS - 232 and RS - 485
used for layer 1 and 2

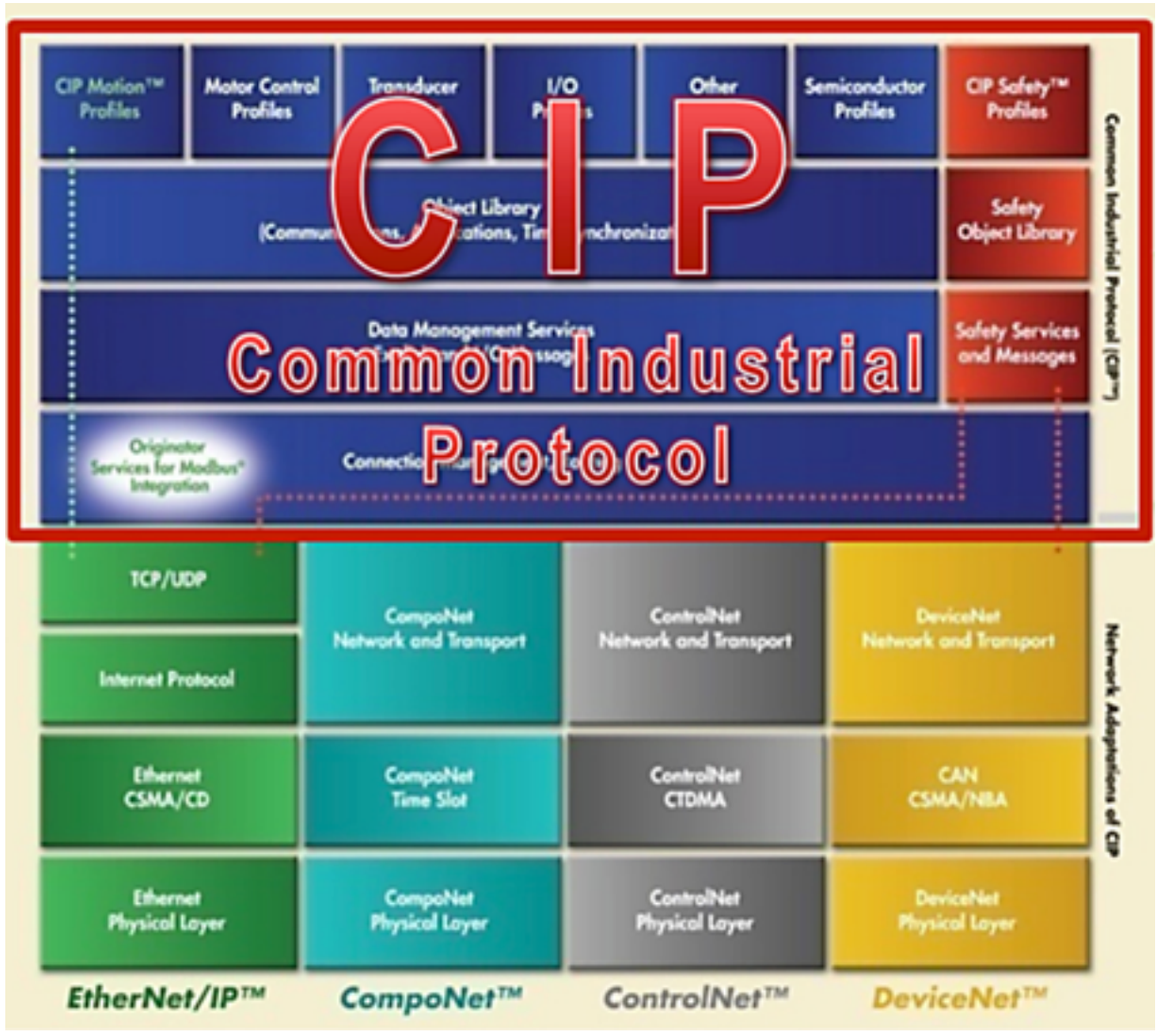
MODBUS/TCP
Maps to layer 1-4 of OSI

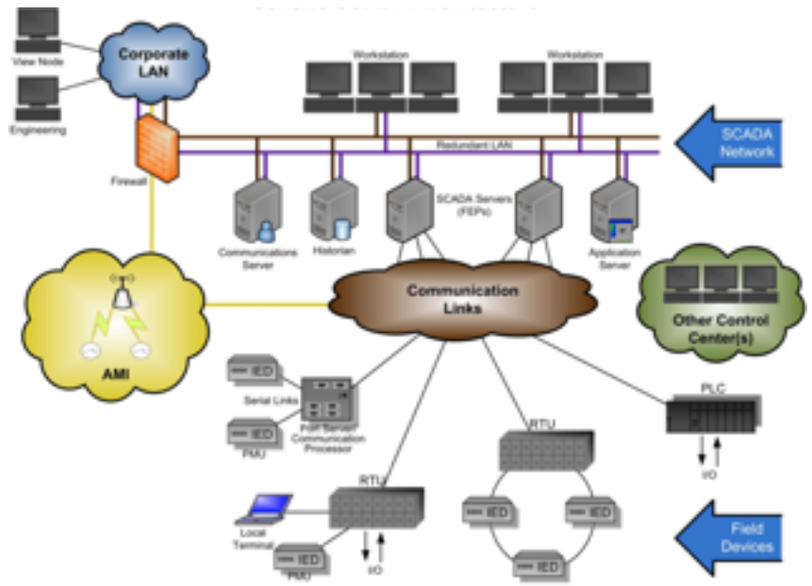
Ethernet II used for layer 1 and 2

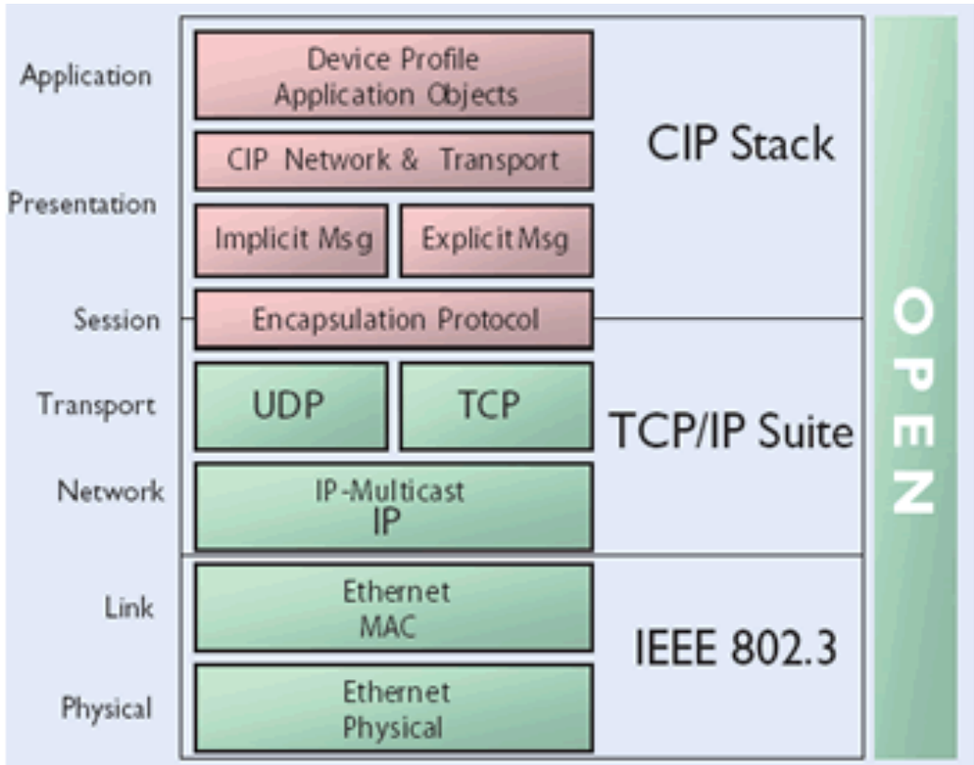
SCADA - ARCHITECTURE

ALGONQUIN COLLEGE

Communications







Common Industrial Protocol

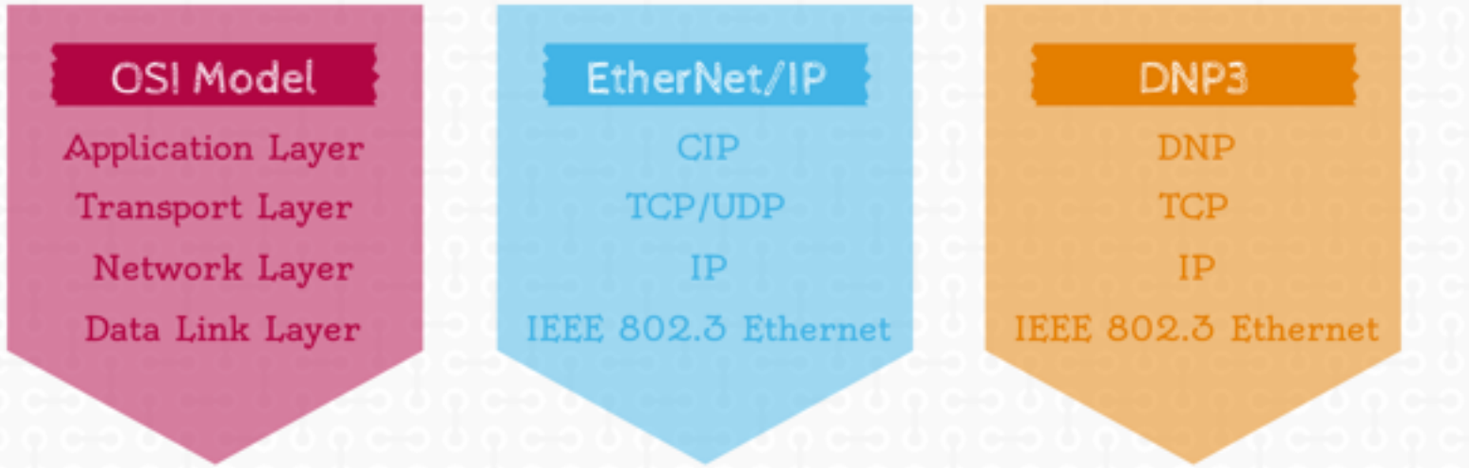
Maps to Layer 5 - 7

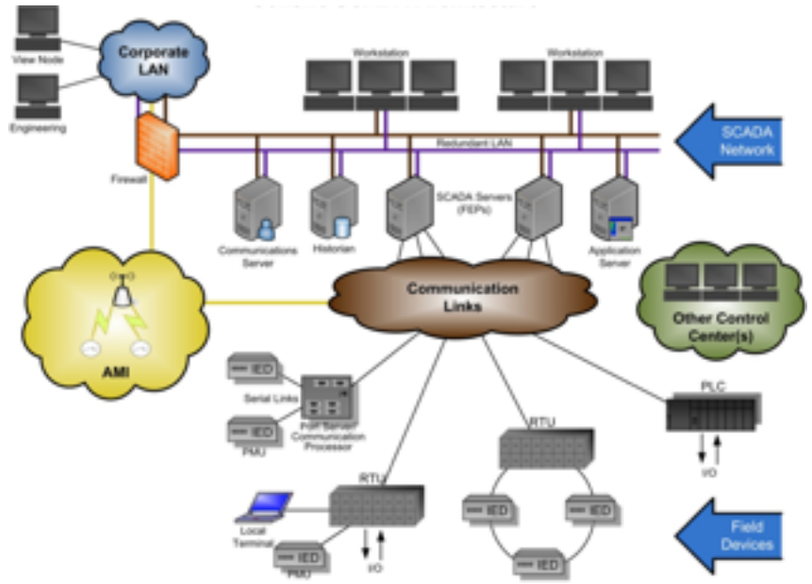
EtherNet/IP used for layer 1 and 2

SCADA - ARCHITECTURE

ALGONQUIN COLLEGE

Communications



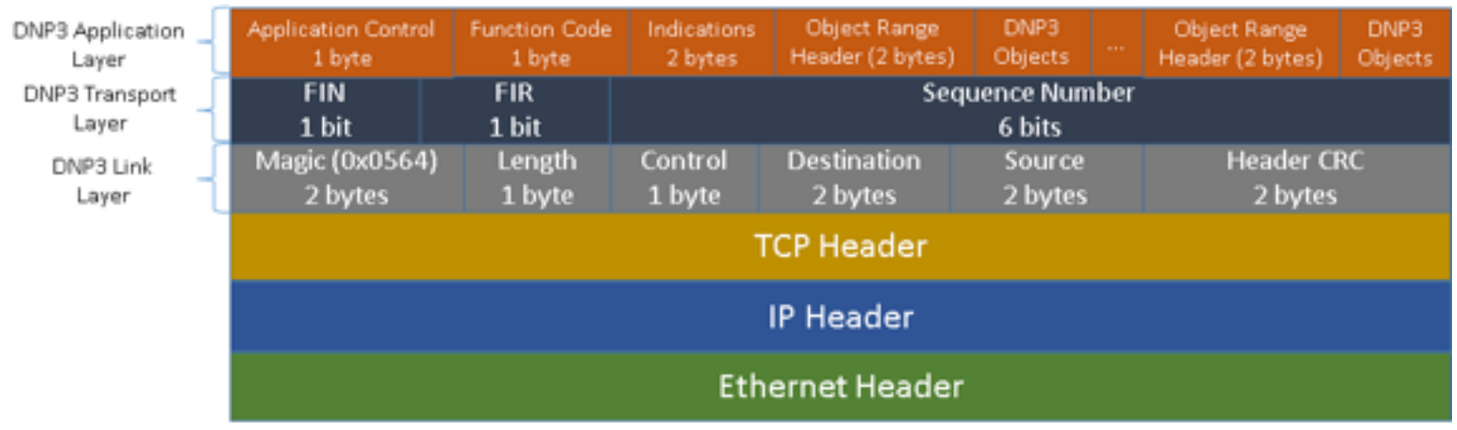


DNP3

Maps to Layer 5 - 7

Ethernet II used for layer 1 and 2

TCP/IP layers 3 and 4 carry the data



SCADA - ARCHITECTURE

ALGONQUIN COLLEGE

Communications

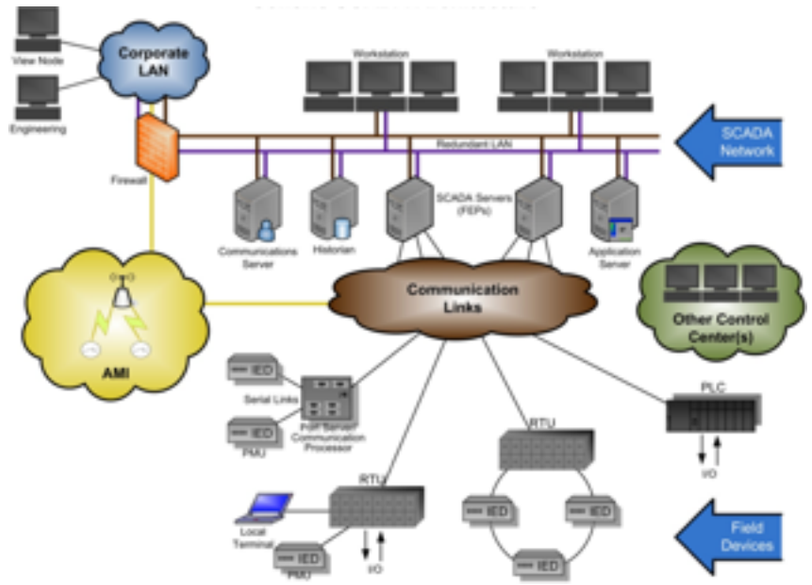
DNP3

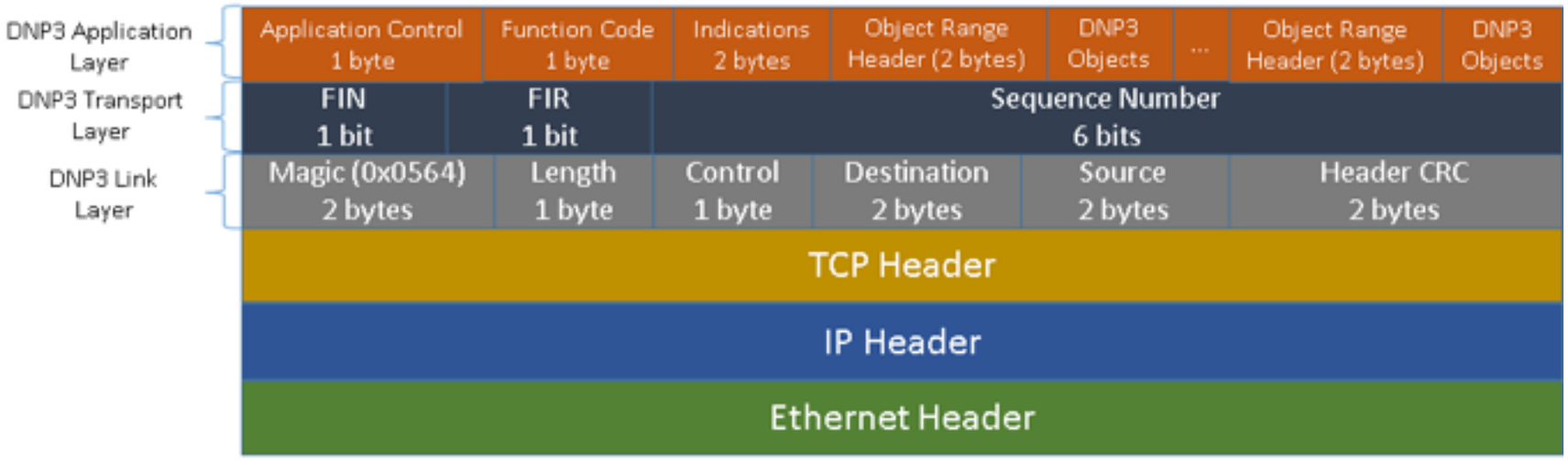
Uses Layers 5 -7

Communication abstracted like the OSI

Makes it very robust and error free

Timestamps are built into the DNP3 Objects





SCADA - ARCHITECTURE

ALGONQUIN COLLEGE