University of Idaho

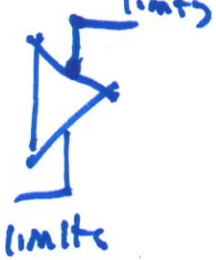
ECE 444 / ECE 544 / CS 444 / CS 544 Supervisory Control and Critical Infrastructure Systems

Session 21

Limits

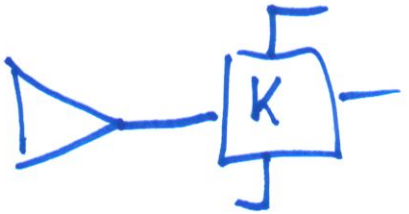
(non-windup limited)

Dynamic Limits



windup limited

static limits



lower limit

Programmable Logic

- discrete logic circuits
  - Latches / Flip Flops
  - PLA, PAL ...
  - → Complex programmable logic devices (CPLDs)
  - Field Programmable gate arrays (FPGA)

programmable systems on ch. p

(Program hardware connections)

- Verilog / VHDL
- moderns have processor core(s)

How do they compute?

- Move bit patterns around
  - Data
    - process data — information
- Why bits (and not analog signals) ?
  - Noise immunity
    - → Data is stable (immutable) as it goes through steps/levels
  - Universal formats
    - ASCII
    - Unicode (16 bit)
  - Good enough for the task

11/2 L21

Numbers, money, pixels, etc....

- Enormous (and growing) infrastructure to manage, process, transmit bits – Digital
  - tools
  - bits are bits → application specific hardware not as common
  - hardened equipment for industrial environment

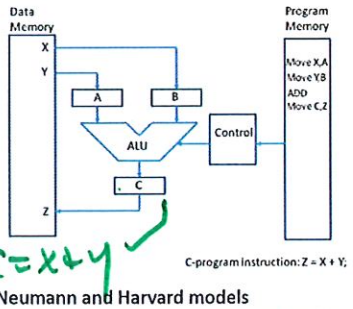
Processor Implementation:

- Universal stored program computer

ALU – arithmetic logic unit

SISO single input single output

Sequential Stored Program Computer Architecture



C = x + y

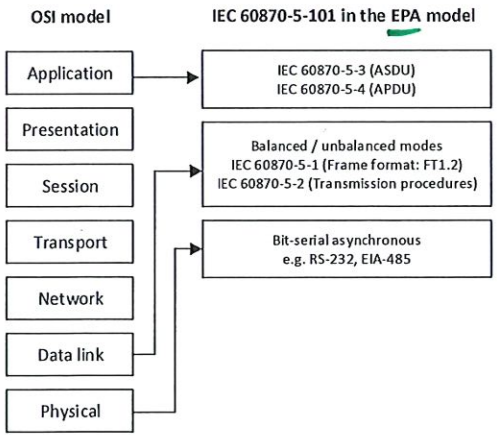
Von Neumann and Harvard models
Fetch and execute instructions sequentially.

11/3/21

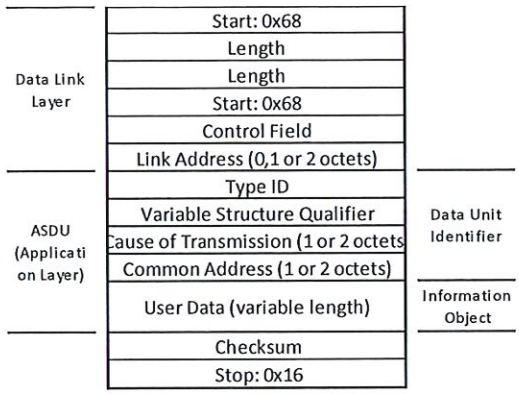
SCADA Protocols IEC 60870-5

- IEC 60870-5 is a collection of standards for SCADA
  - » DNP3 was developed at same time – out of draft version
- IEC 60870-5-101
  - » Serial over low bandwidth channel
  - » First version in 1994 – called T101
- IEC 60870-5-104
  - » Specifies the TCP/IP suite in the network and transport layers to provide LAN or WAN operation
  - » Added in 2000

IEC 60870-5 in OSI Model

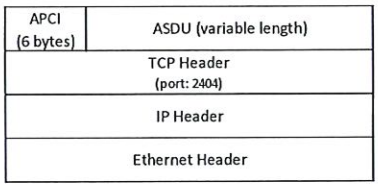


T101 Message Format

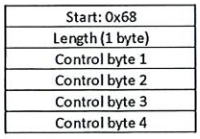


T104 in TCP/IP

- Defines network operation of T101 over TCP/IP



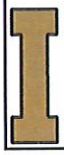
- Application Protocol Control Information (ACPI) is a control field



11/5 L21

SCADA Protocols: MODBUS

- Created in 1970's by Modicon
  - » Has passed through several owners over the years
  - » Initial developed for PLC
  - » Widespread use made it a de-facto standard
- https://modbus.org



SCADA Variants

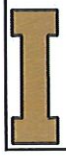
- MODBUS ASCII
  - » ASCII symbols
- MODBUS RTU
  - » Binary digital data messages - serial
- MODBUS Plus
  - » Extension from one group – not widely used - design for Token Ring
- MODBUS TCP/IP
- MODBUS UDP - universal datagram protocol

SUNSPEC MODBUS - specific to PV inverters

11/9 12:7

MODBUS Pros

- Easy to read/troubleshoot
- Has server device addressing
- Has built-in data integrity checking (CRC)
- Readily available on most devices
- Since sent over physical media can observe traffic to troubleshoot
  - » Serial COM port sniffer
  - » Wireshark or similar TCP/IP or UDP



MODBUS Pros and Cons

- Pros
  - » Easy to read/troubleshoot
  - » Has server device addressing
  - » Has built-in data integrity checking (CRC)
  - » Readily available on most devices
- Cons
  - » Message start/start all time based
  - » Does not have client device addressing
  - » Message size limitations slows updates, especially on serial channels
  - » No data quality, timestamps without adding special logic
  - » While TCP/IP security is available, not commonly used

secure variant of MODBUS

1/2 127

Time Synchronized Phasor Measurements

CS&ECE 444/544

Lecture 21

- What is a "synchrophasor"?
  - » A synchrophasor is a phasor measurement with respect to an absolute time reference.
  - » Allows determination of absolute phase relationship between quantities at different locations in a power system

First, how do we define a phasor?

CS&ECE 444/544

Lecture 21

- start from sinusoidal waveform
- magnitude V_m
- angle θ_V
- frequency ω

$v(t) = V_m \cos(\omega t + \theta_V)$

$|V| \angle \theta_V$

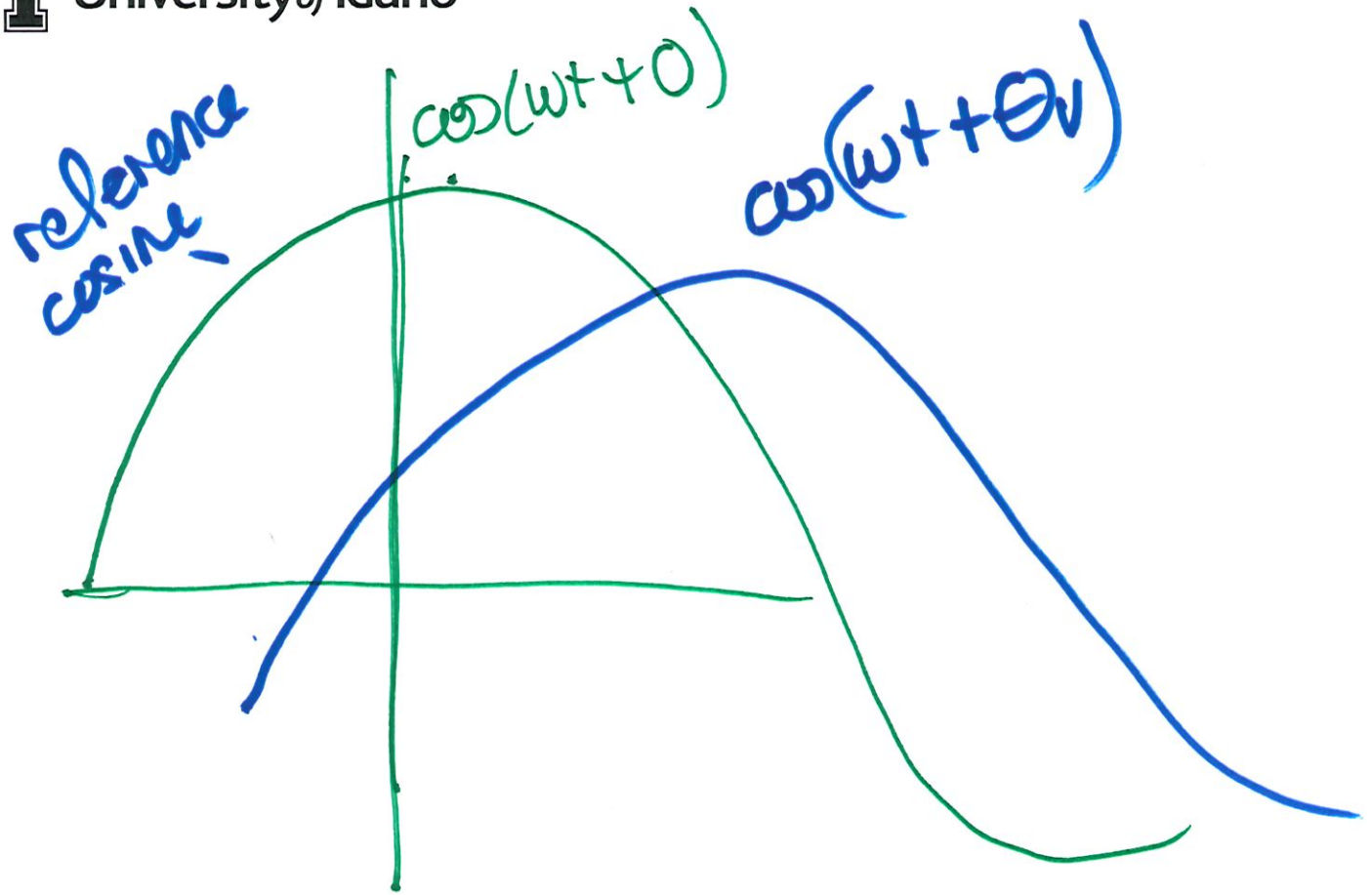
$= |V| e^{j\theta_V}$

$= |V| (\cos\theta_V + j \sin\theta_V)$

Euler's identity

$|V| = \frac{V_m}{\sqrt{2}}$

θ_V is a relative angle compared to a reference


reference cosine
cos(ωt+θ)
cos(ωt+θv)

In a meter or protective relay

- one measurement is assigned as a reference
  - angles of other variables are relative to that reference
- usually reference is a voltage

Reference Angle is not too Difficult in a Substation

CS&ECE 444/544

Lecture 21

- common clock reference to all devices in the station
  - IRIG-B
- could define a reference for all measurements in station

3

→ How about substation to substation?

Benefits of External Reference

CS&ECE 444/544

Lecture 21

- Phadke and Thorpe→ GPS clock signals
- Slow adoption

4

11/1 12:1