Designing a Robust IIoT to SCADA Gateway

Class 1: The Challenges of IIoT and Industrial Ethernet

October 22, 2018

Charles J. Lord, PE
President, Consultant, Trainer
Blue Ridge Advanced Design and Automation

Presented by:

DesignNews

Blue Ridge Advanced Design and Automation
Asheville, North Carolina

CEC CONTINUING EDUCATION CENTER

Digi-Key ELECTRONICS

This Week's Agenda

10/22 The Challenges of IIoT and Industrial Ethernet

10/23 Introduction to the RZ/N1

10/24 Many Protocols, One Abstraction - GOAL

10/25 Programming the R-IN Protocol Engine

10/26 Writing and Testing Our Application

This Week's Agenda

10/22 The Challenges of IIoT and Industrial Ethernet

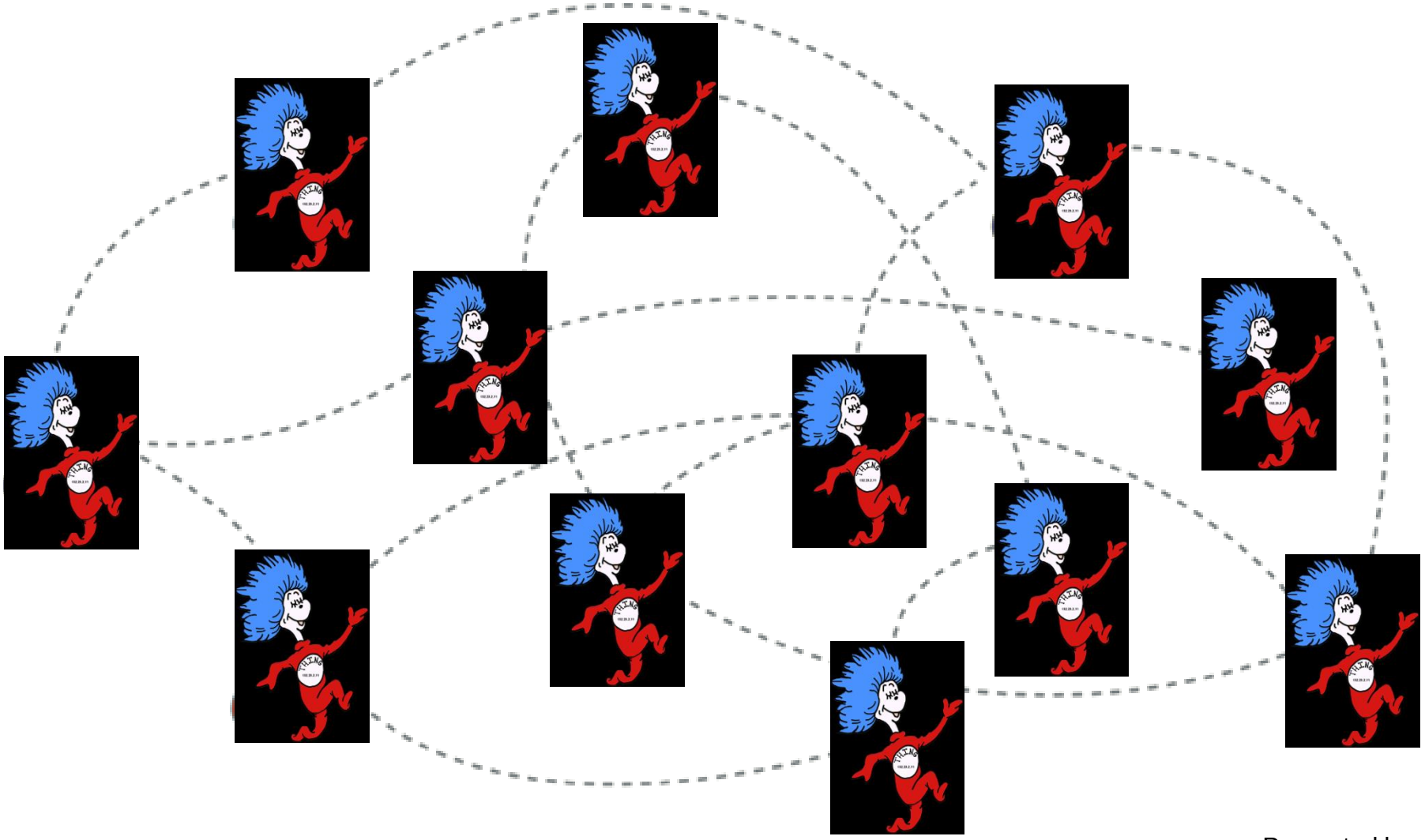
10/23 Introduction to the RZ/N1

10/24 Many Protocols, One Abstraction - GOAL

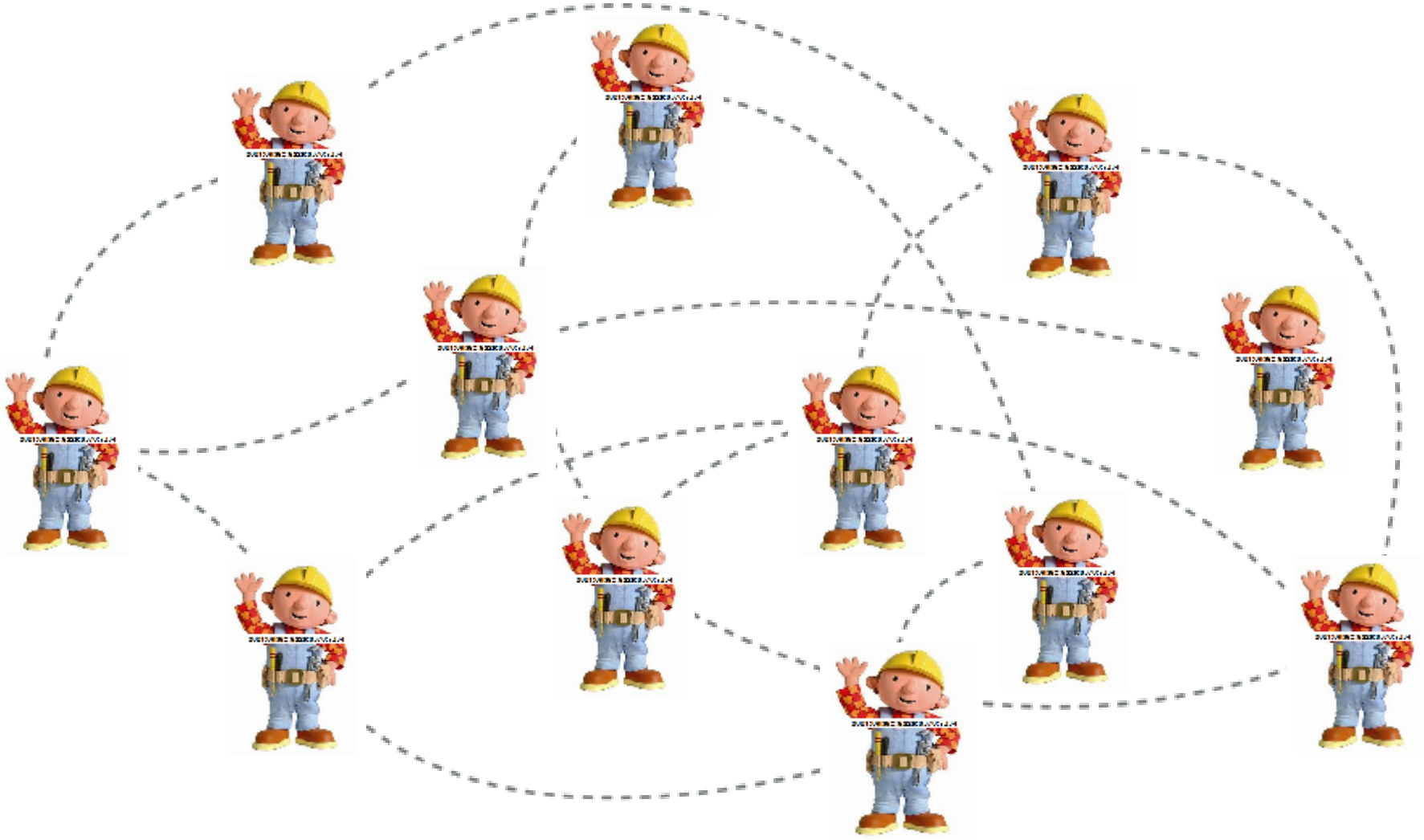
10/25 Programming the R-IN Protocol Engine

10/26 Writing and Testing Our Application

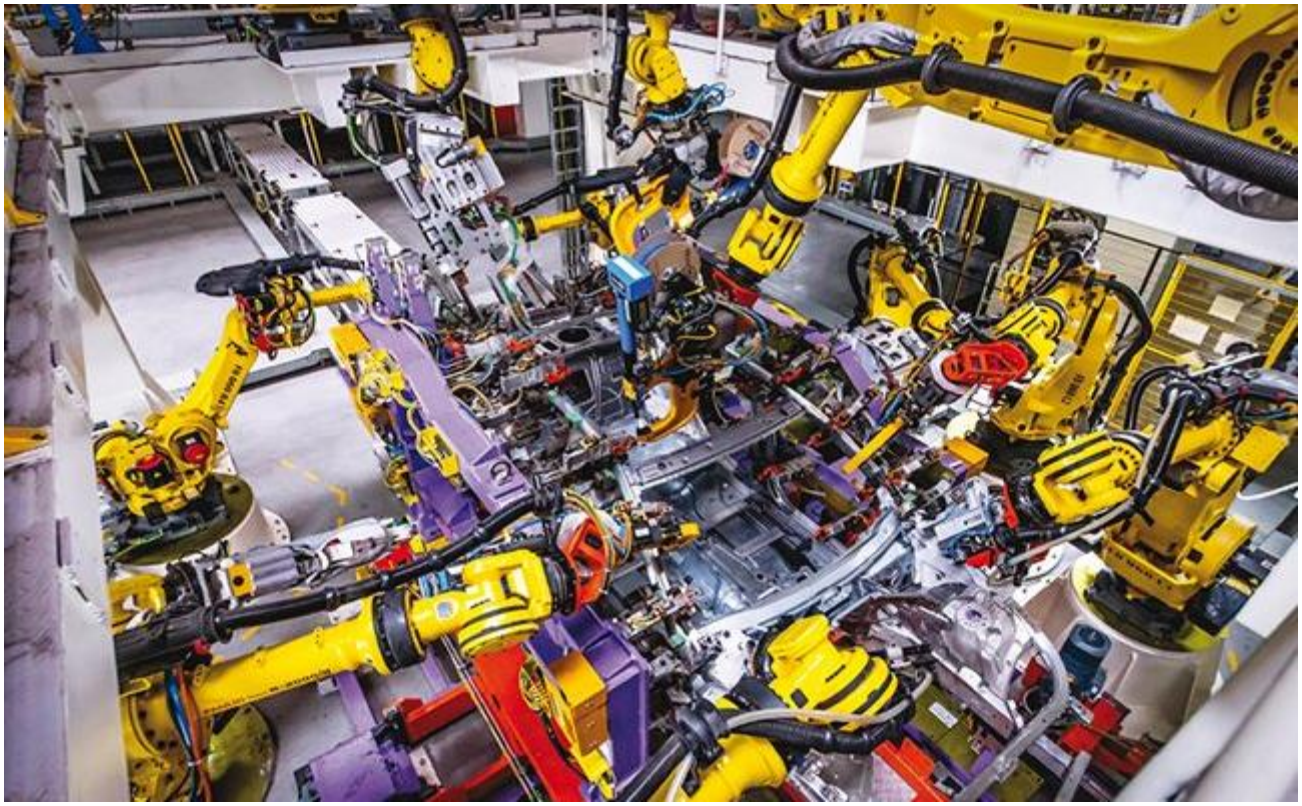
Internet of Things



Industrial Internet of Things

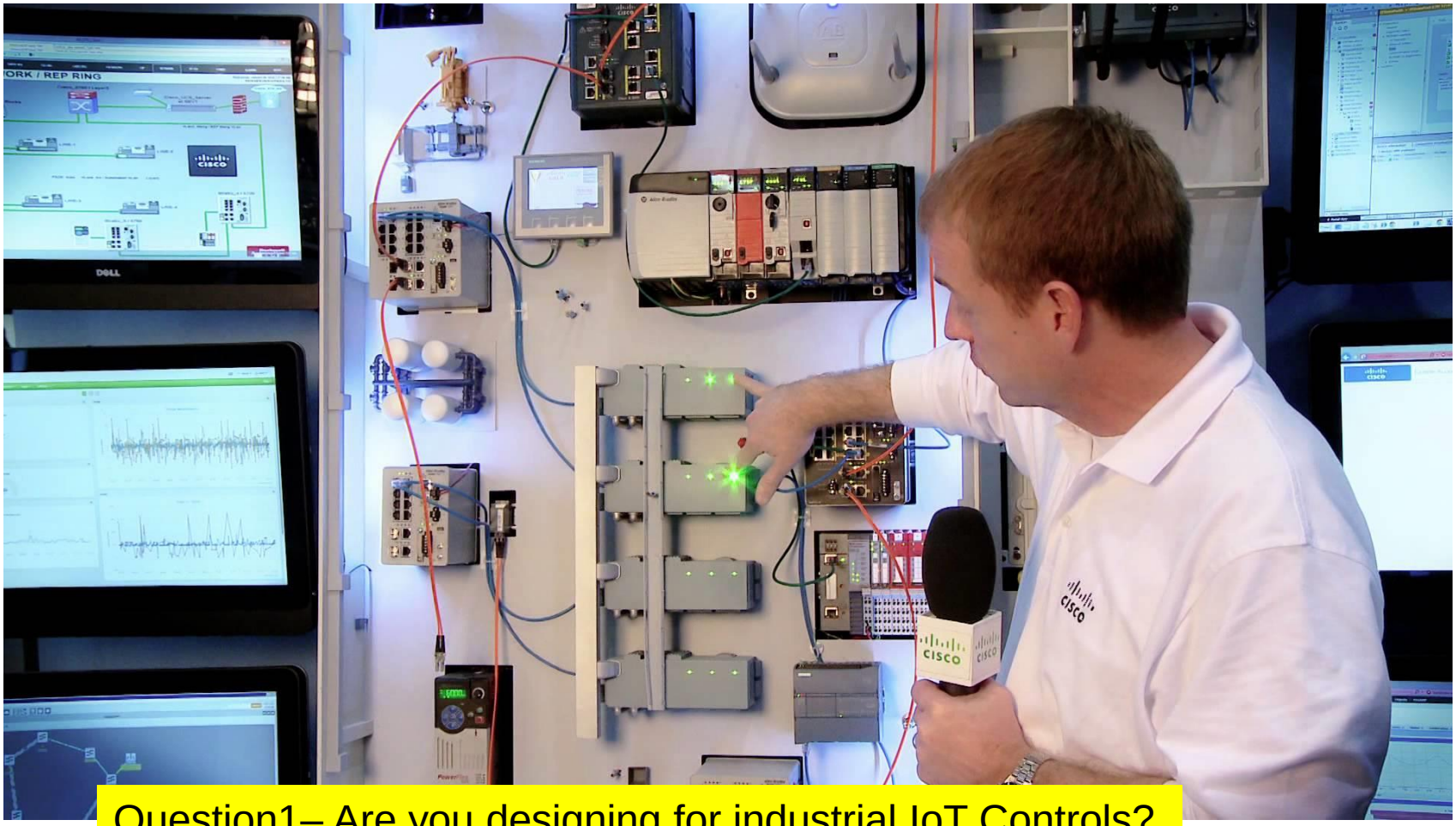


Factory Automation



The Connected Factory

An Example from Cisco



Question1– Are you designing for industrial IoT Controls?

The ABC's of the IIoT

- SCADA
- PLC
- CAN
- RS-485
- Deterministic
- Current Loop
- Ethernet
- PROFINET
- PROFINET IRT
- EtherCAT
- Modbus
- SERCOS III

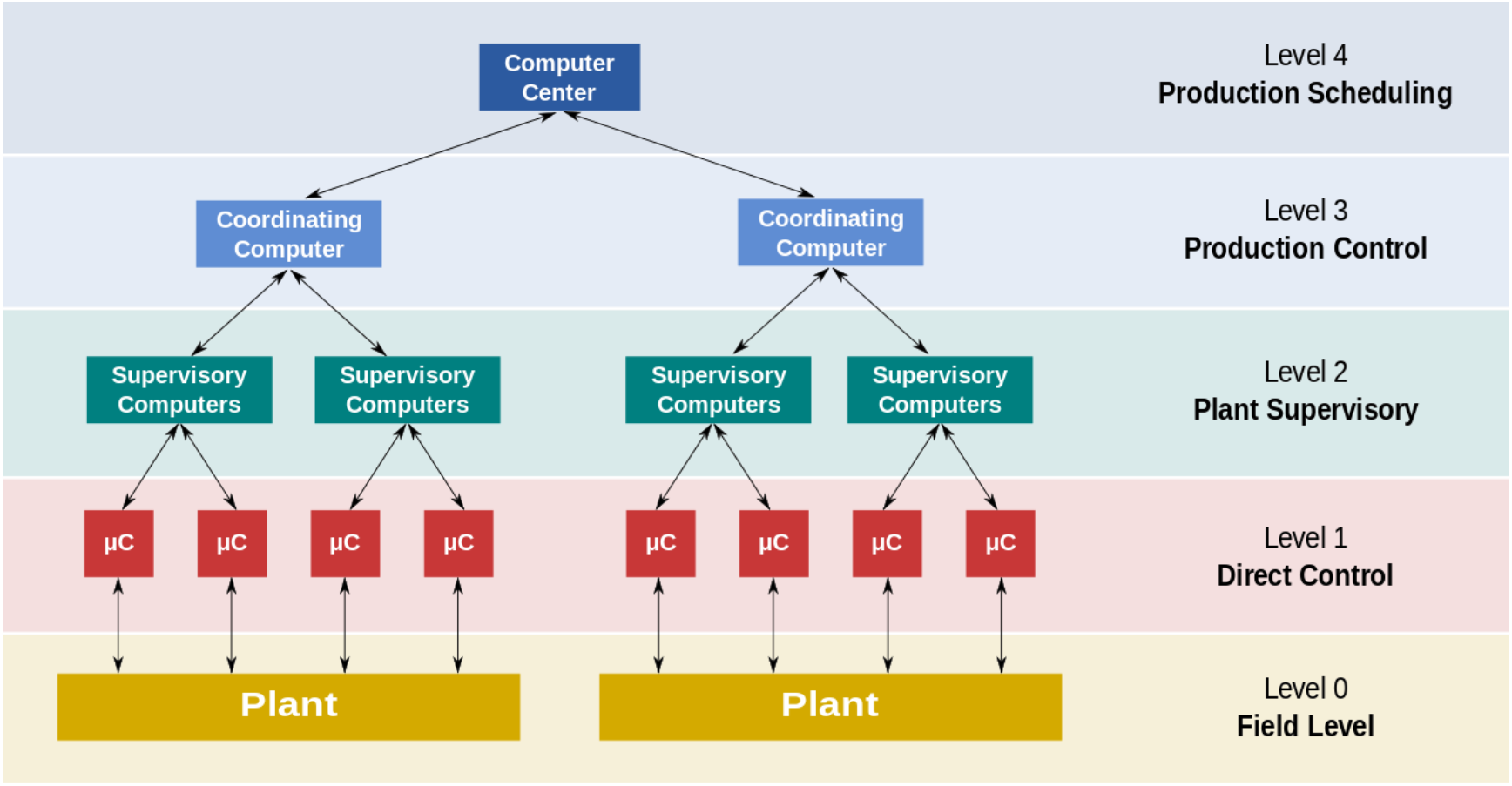
SCADA

Supervisory control and data acquisition (SCADA) is a control system architecture that uses computers, networked data communications and graphical user interfaces for high-level process supervisory management, but uses other peripheral devices such as programmable logic controller (PLC) and discrete PID controllers to interface with the process plant or machinery.

The operator interfaces which enable monitoring and the issuing of process commands, such as controller set point changes, are handled through the SCADA computer system.

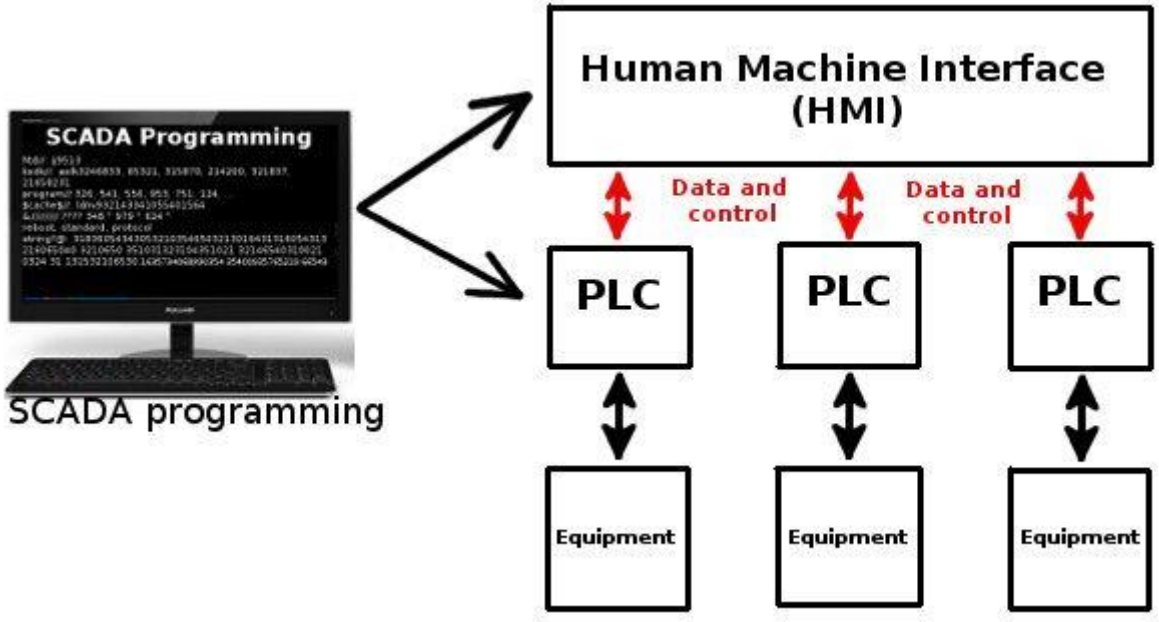
Real-time control logic or controller calculations are performed by networked modules which connect to the field sensors and actuators.

The Layers of SCADA



Wikipedia CC by Daniele Pugliesi

Simplified SCADA



PLC

- A programmable logic controller (PLC) or programmable controller is an industrial digital computer which has been ruggedized and adapted for the control of manufacturing processes, such as assembly lines, or robotic devices, or any activity that requires high reliability control and ease of programming and process fault diagnosis.

PLCs

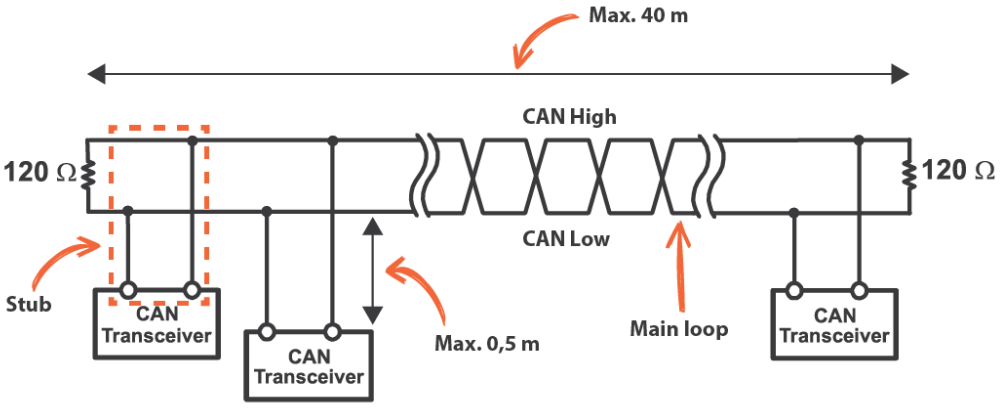

Eurotherm
F1
F2
F3
F4
E+PLC

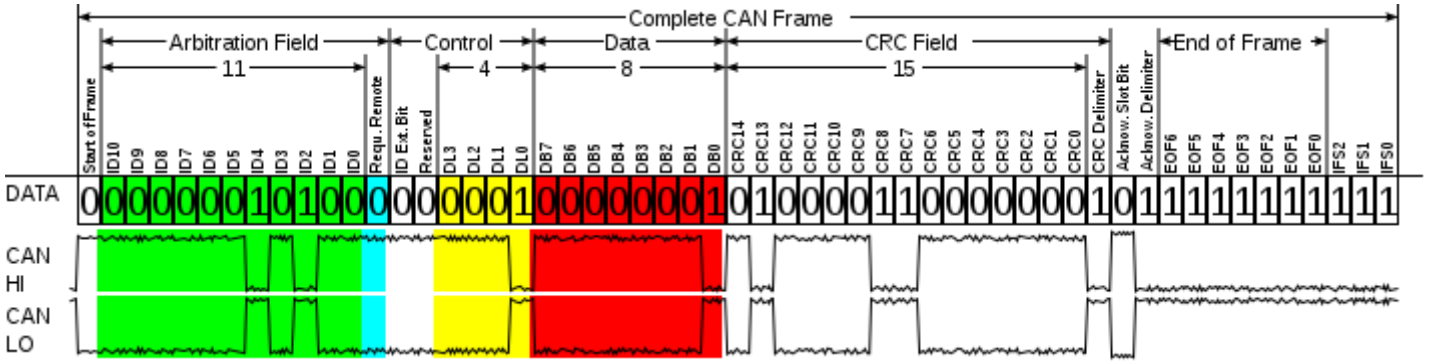

ABB
CM588
PM591
AC500
WARNING
AX522
AI523

CAN

- A Controller Area Network (CAN bus) is a robust vehicle bus standard designed to allow microcontrollers and devices to communicate with each other in applications without a host computer. It is a message-based protocol, designed originally for multiplex electrical wiring within automobiles to save on copper, but is also used in many other contexts

CAN Interface





RS-485

- Serial interface which is an outgrowth of RS-232 but with differential pair in NRZ
- Longer runs
- Higher noise immunity
- Multi-drop
- Standard in lighting controls, vending applications, PLCs

Current Loop

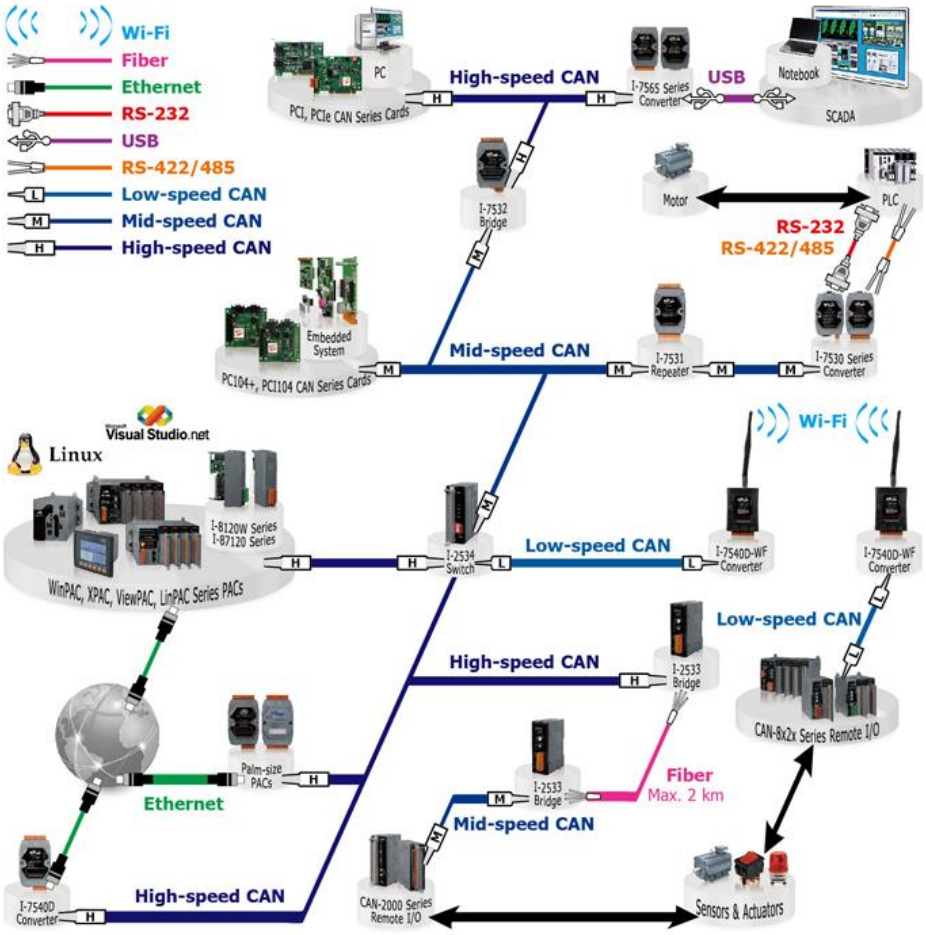
- Signals 0 and 1 by changing current through a closed loop from 4mA to 20mA
- One of the earliest signaling protocols
- Can also transmit analog signals
- LOW speed, moderate noise immunity
- Only needed for legacy equipment – but still out there! (mostly in analog)

Question 2 – Working with any current loop sensors or other equipment?

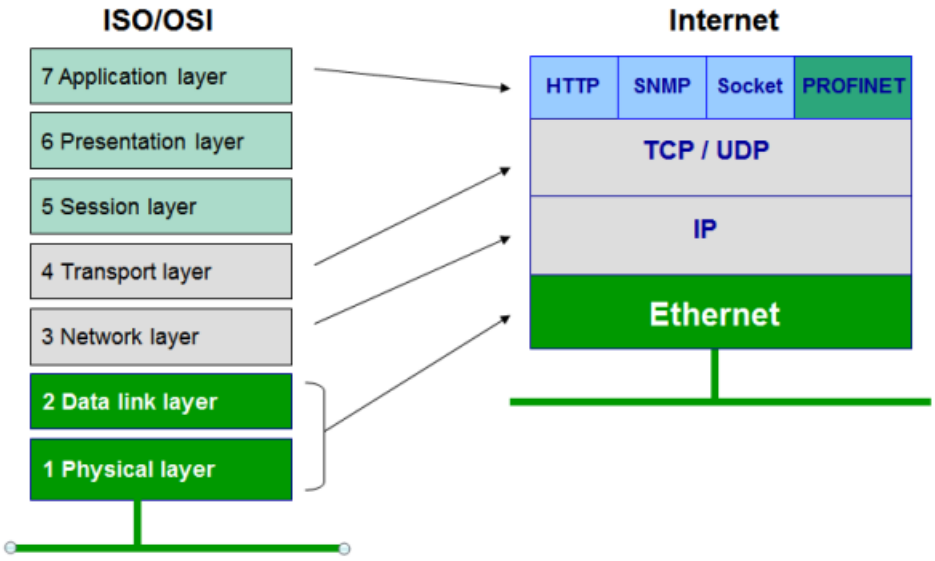
Deterministic

- Industrial Controls are characterized by absolutes in timing, error handling, and other parameters
- Rather than IT principles of security and “wait until it’s right,” IIoT is also driven by Operational Technology – things have to monitor and act in specific timing, and without delay
- Timing is a critical element

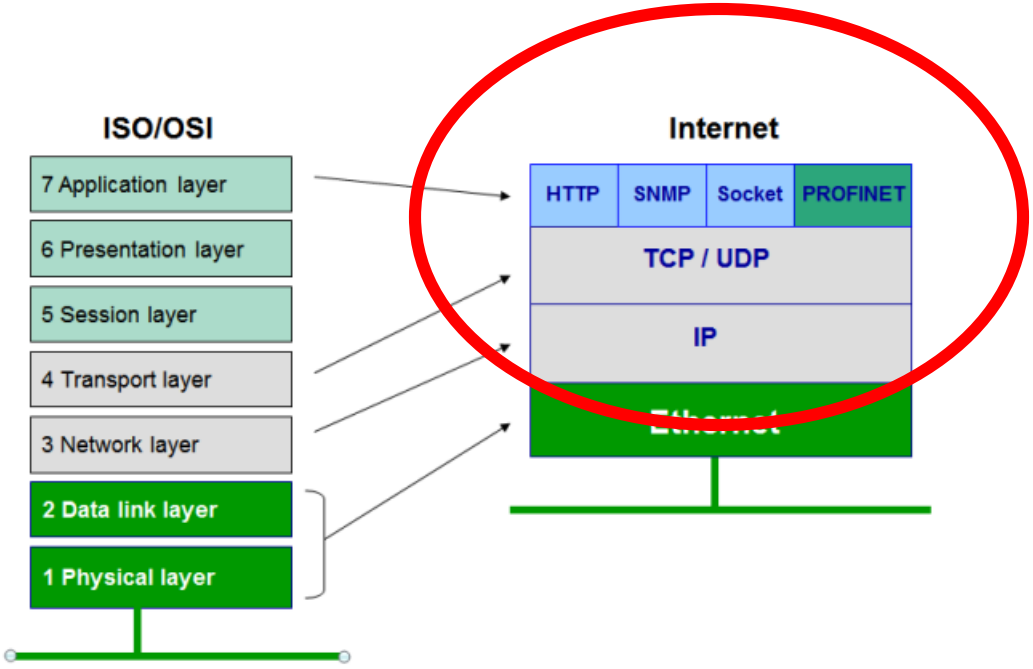
About that Ethernet…



Ethernet is just the Link-Layer



What's Important is What Goes on Top



Internet Protocol

- The basics of wired IP (v4 or v6) is that it is still a CSMA/CD (Carrier Sense Multiple Access/Collision Detect) protocol, as opposed to 802.11 networks which use CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance).
- Basic Ethernet has no provision for accurate timing of packets
- Enter the Precision Time Protocol (IEEE-1588)

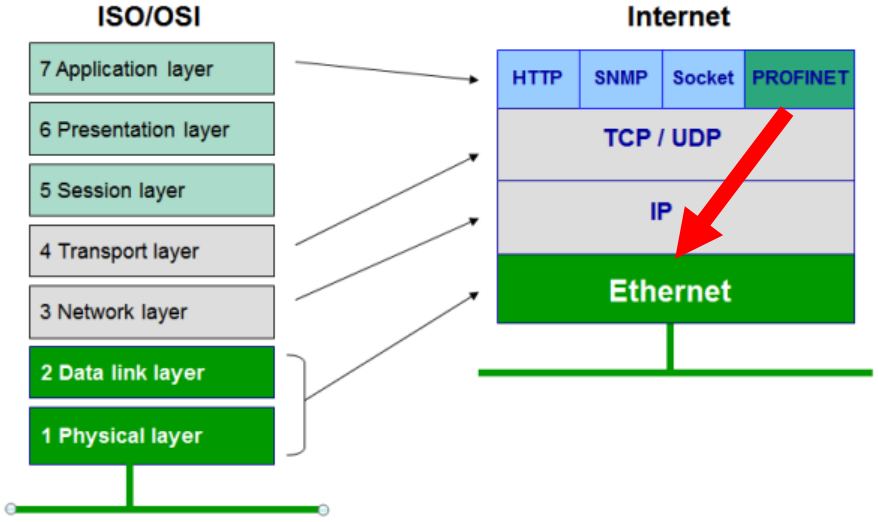
How to “Fix” Ethernet for Industrial Controls

- Many competing buses exist for Ethernet connectivity in industrial controls. Unless one has control of the devices that are part of a SCADA system in our IIoT solution, we should be capable of working with multiple protocols, all the while maintaining the real-time operation of the system
- Let’s look at some of those protocols…

Question 3 – Are you using any of the following buses?

PROFINET

- Profinet eliminates some of the timing issues of the TCP or UDP handshaking by replacing the third and fourth layers and effectively becoming an ICMP (Internet Control Message Protocol)



Provides accurate cycle times as short as 1 millisecond and jitter of about 10-100µs

When “Real-Time” Isn’t Good Enough

- In tightly controlled, deterministic systems, even the accurate timing of PROFINET isn’t good enough. Delays, collisions, and jitter can cause the asynchronous media access control (MAC) layer to fail.
- PROFIBUS-IRT adds Isochronous Real-Time (IRT) Communication as a modification of the MAC layer. Dedicated time slots carry only IRT traffic so that it cannot be affected by other traffic. ‘Normal’ Ethernet traffic is allowed outside those slots.

EtherCAT

- EtherCAT (Ethernet for Control Automation Technology) is an Ethernet-based fieldbus system, invented by Beckhoff Automation. The protocol is standardized in IEC 61158 and is suitable for both hard and soft real-time computing requirements in automation technology.
- Based on a modified MAC structure, similar to token ring

SERCOS III

- Third generation Serial Realtime Communication System (SERCOS) designed to operate over Ethernet
- Similar to PROFINET-IRT, establishes dedicated time slots for synchronous traffic
- Eliminates hubs and switches to avoid extra delays
- Typically needs custom hardware inferface

Modbus

- Modbus is a standard fieldbus protocol that bridges both serial (RS-485 and even RS-232) and Ethernet-based systems
- Originally developed for serial, it now has two variants that use Ethernet lines:
  - Modbus TCP/IP or Modbus TCP —Modbus variant used for comms over TCP/IP networks, counting on lower layers already provide checksum protection.
  - Modbus over TCP/IP or Modbus over TCP or Modbus RTU/IP — This is a Modbus variant that differs from Modbus TCP in that a checksum is included in the payload.

Welcome to the United Nations

- We need a way to properly deal with these different protocols
- A common Ethernet PHY can handle our interface, but we need absolute real-time communications and control for each port
- Tomorrow, we will look at an innovative multiprocessor chip that is designed to handle these tasks (as well as our application)

This Week's Agenda

10/22 The Challenges of IIoT and Industrial Ethernet

10/23 Introduction to the RZ/N1

10/24 Many Protocols, One Abstraction - GOAL

10/25 Programming the R-IN Protocol Engine

10/26 Writing and Testing Our Application

Please stick around as I answer your questions!

- Please give me a moment to scroll back through the chat window to find your questions
- I will stay on chat as long as it takes to answer!
- I am available to answer simple questions or to consult (or offer in-house training for your company)
  c.j.lord@ieee.org
  http://www.blueridgetechnc.com
  http://www.linkedin.com/in/charleslord
  Twitter: @charleslord
  https://www.github.com/bradatraining