RSAConference2018
San Francisco | April 16–20 | Moscone Center

SESSION ID: SBX4-R3

SCADA 101

Johnny Xmas

Security Researcher
Uptake
@j0hnnyxm4s

Adam Ringwood

Security Researcher
Uptake
@avidhacker

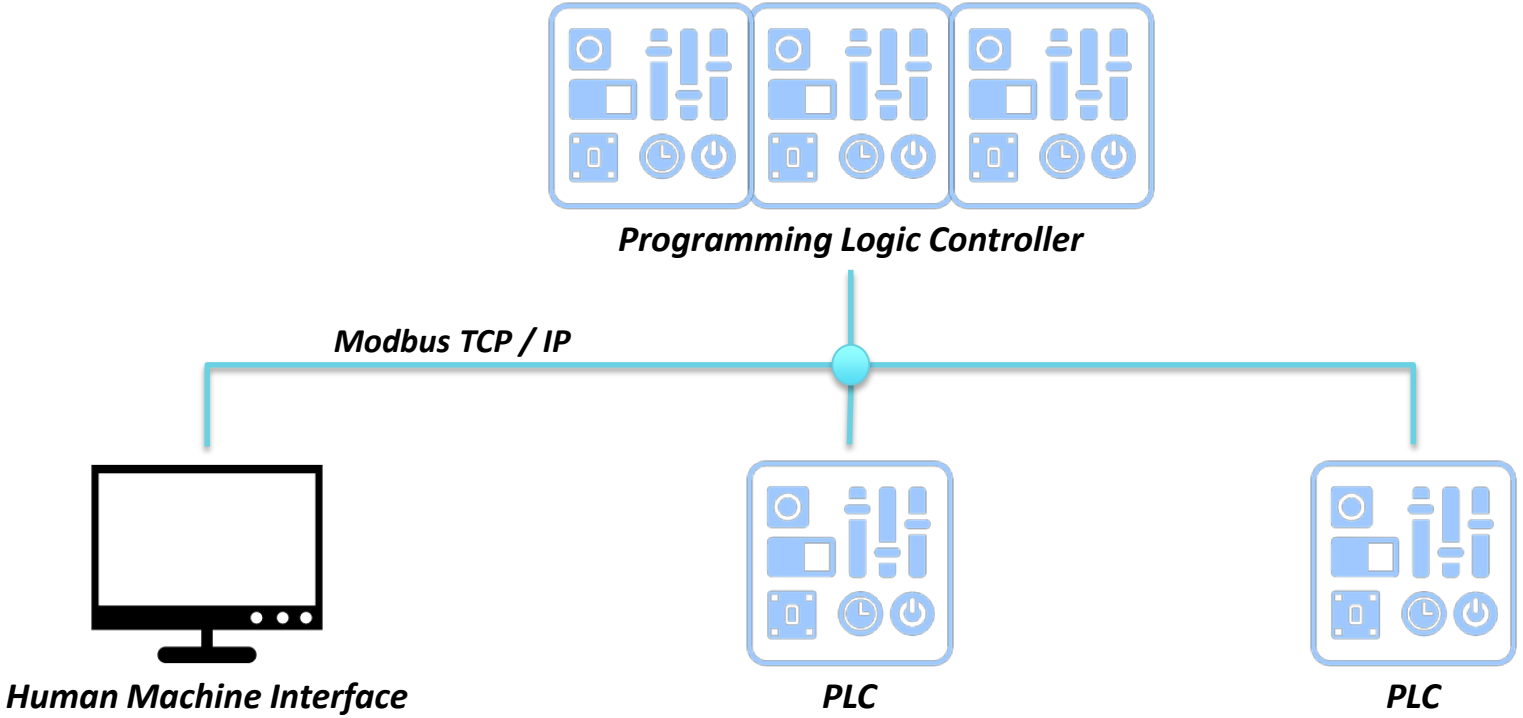
OPERATIONAL TECHNOLOGY OVERVIEW

IT versus OT

- Windows & *nix Servers
- Ethernet Networking Equipment
- Laptops & Desktops
- TCP / IP

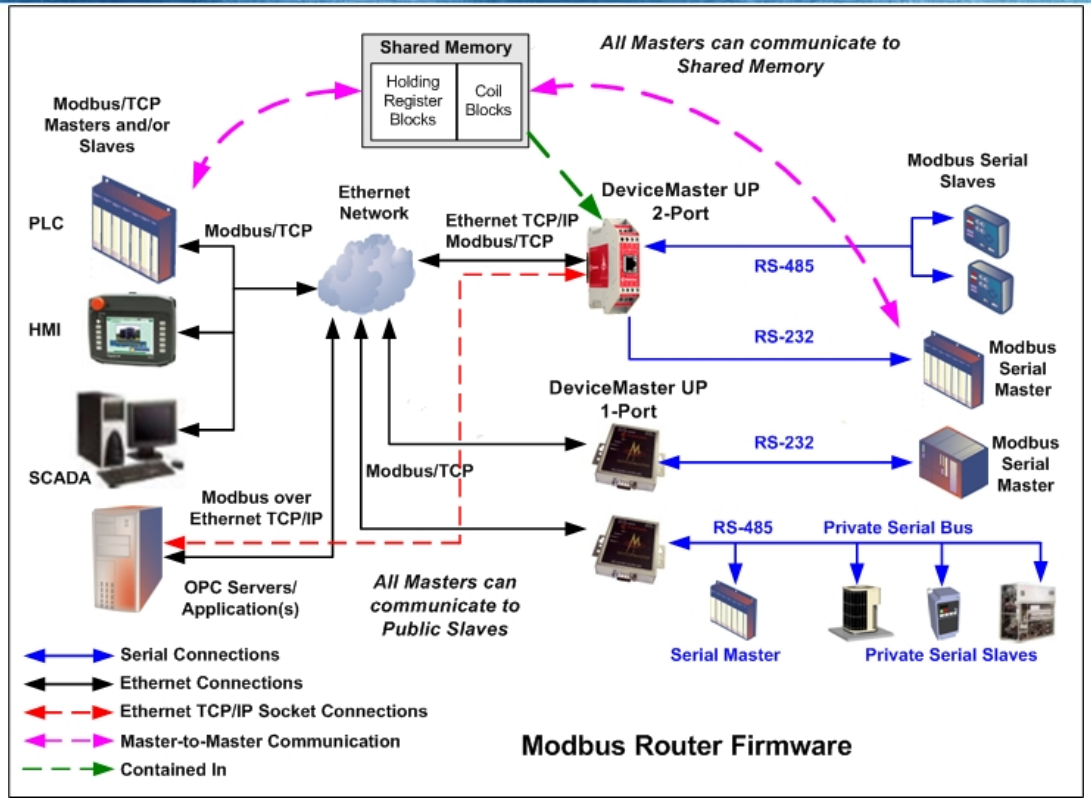
- Electromechanical Equipment
- Real-time Operating Systems
- Simple CPUs
- SCADA & Other Comms

HMIs & PLCs

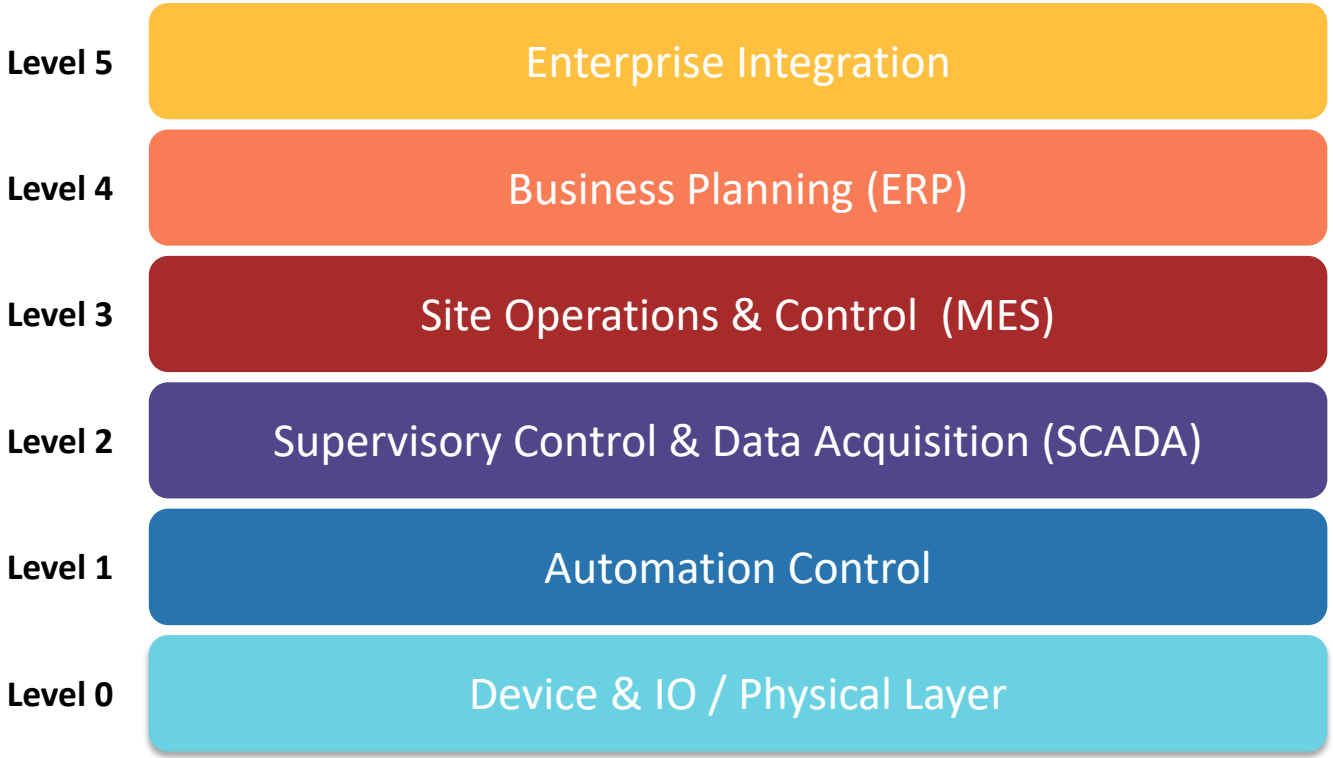

Programming Logic Controller
Modbus TCP / IP
Human Machine Interface
PLC
PLC

COMMUNICATION METHODOLOGY

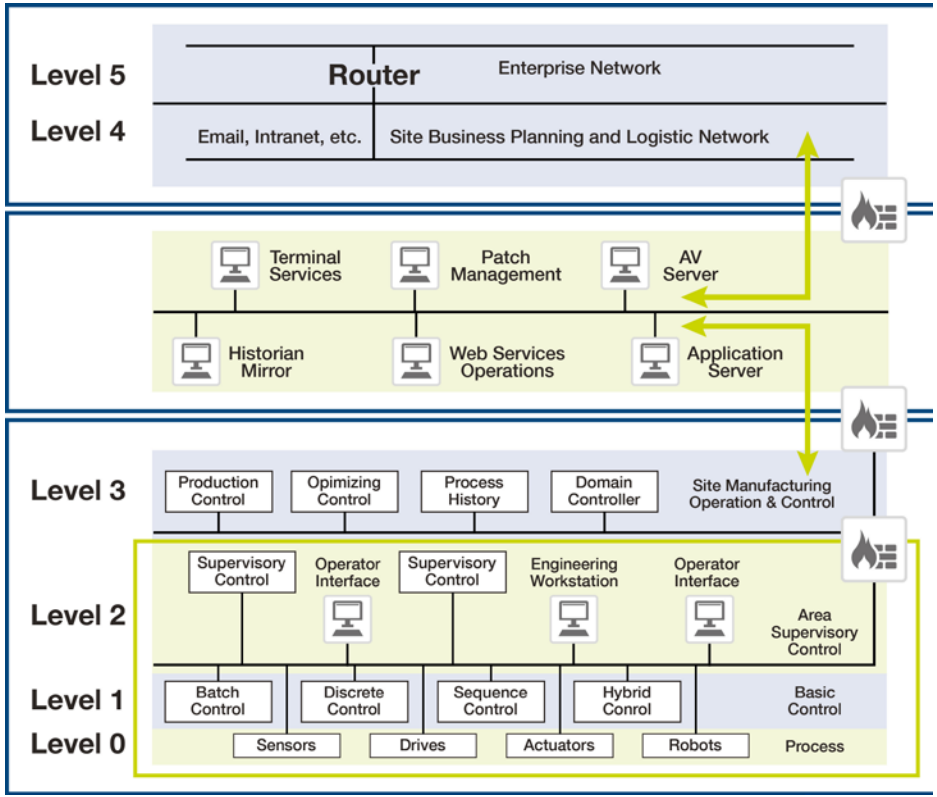
Communication Methods



The Purdue Model Simplified

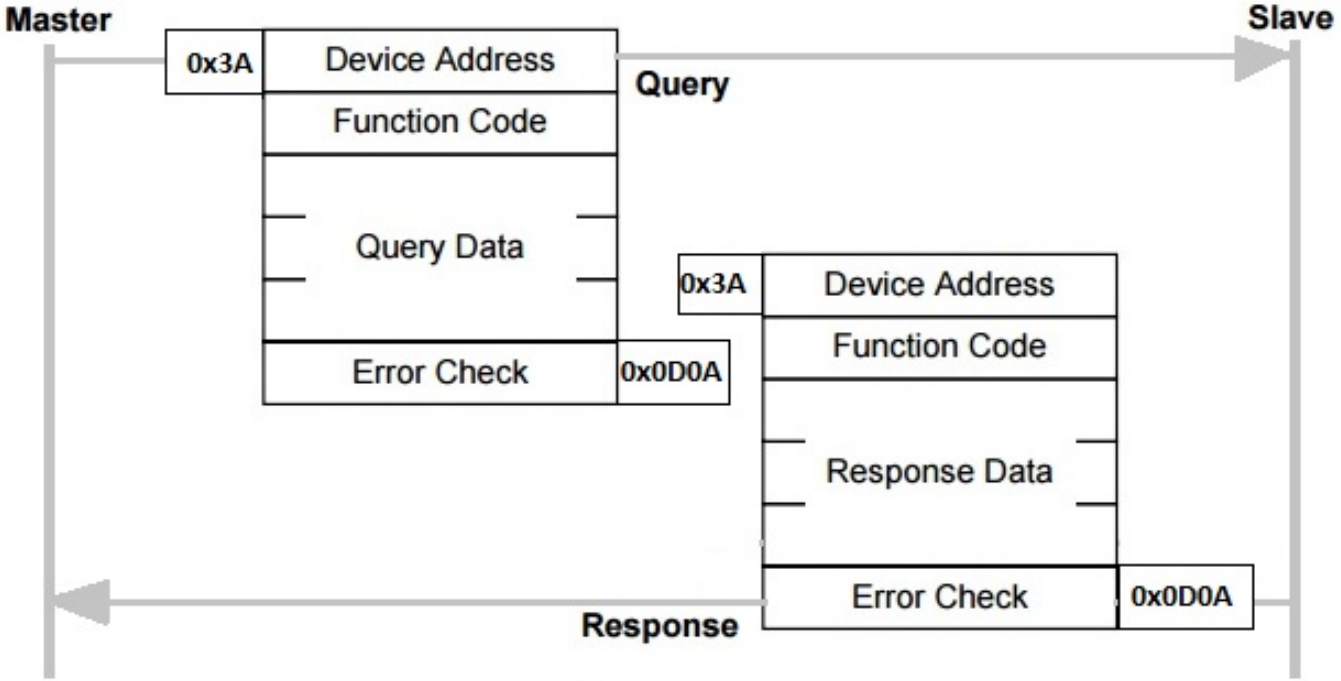


The Purdue Model Detailed



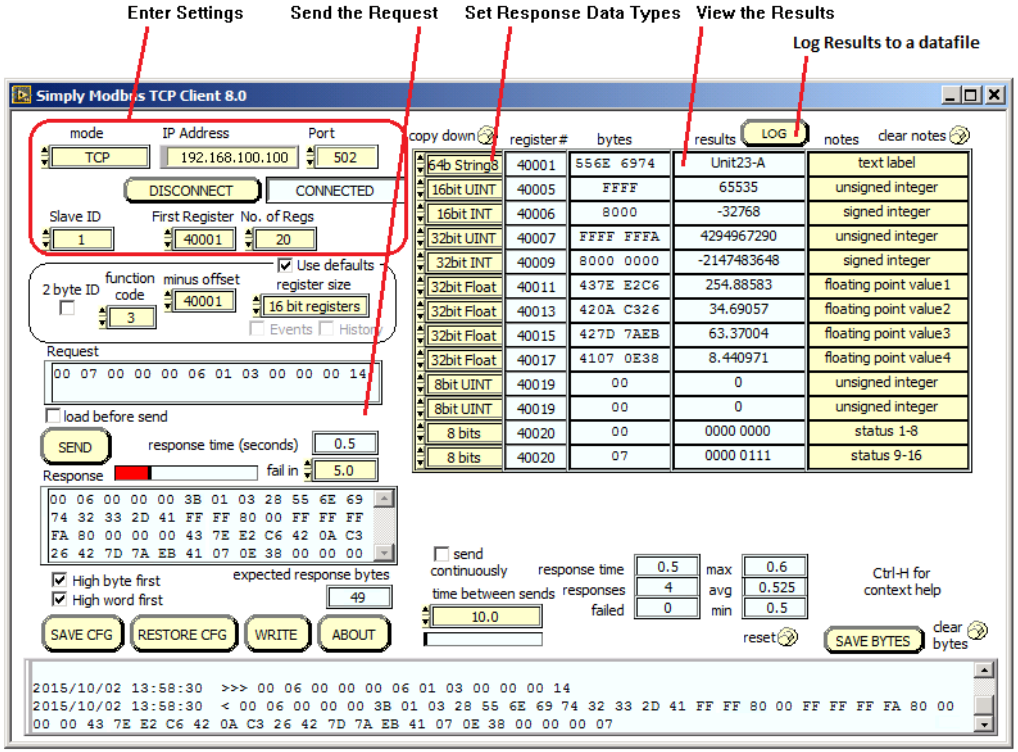
INDUSTRIAL PROTOCOLS

MODBUS (MODicon BUS)



Modbus Message Frames

CIP (Common Industrial Protocol)



LIVE HACK

Live Hacks

- Modbus Set Point Injection
- CIP Replay Attack

RSAConference2018

San Francisco | April 16–20 | Moscone Center

SESSION ID:

THANK YOU

Johnny Xmas

Security Researcher
Uptake
Johnny.Xmas@Uptake.com

Adam Ringwood

Security Researcher
Uptake
Adam.Ringwood@Uptake.com