

RSA® Conference 2018

San Francisco | April 16 – 20 | Moscone Center

SESSION ID: SBX4-R3

SCADA 101



#RSAC

Johnny Xmas

Security Researcher
Uptake
@j0hnnym4s

Adam Ringwood

Security Researcher
Uptake
@avidhacker

RSA® Conference 2018



#RSAC

OPERATIONAL TECHNOLOGY OVERVIEW

IT versus OT

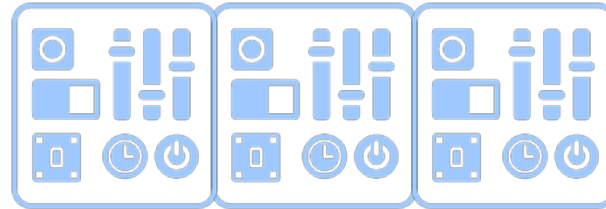


- Windows & *nix Servers
- Ethernet Networking Equipment
- Laptops & Desktops
- TCP / IP



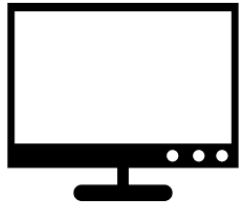
- Electromechanical Equipment
- Real-time Operating Systems
- Simple CPUs
- SCADA & Other Comms

HMIs & PLCs

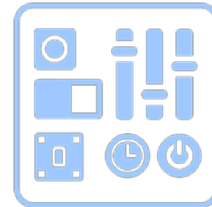


Programming Logic Controller

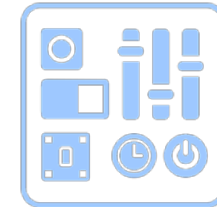
Modbus TCP / IP



Human Machine Interface



PLC



PLC

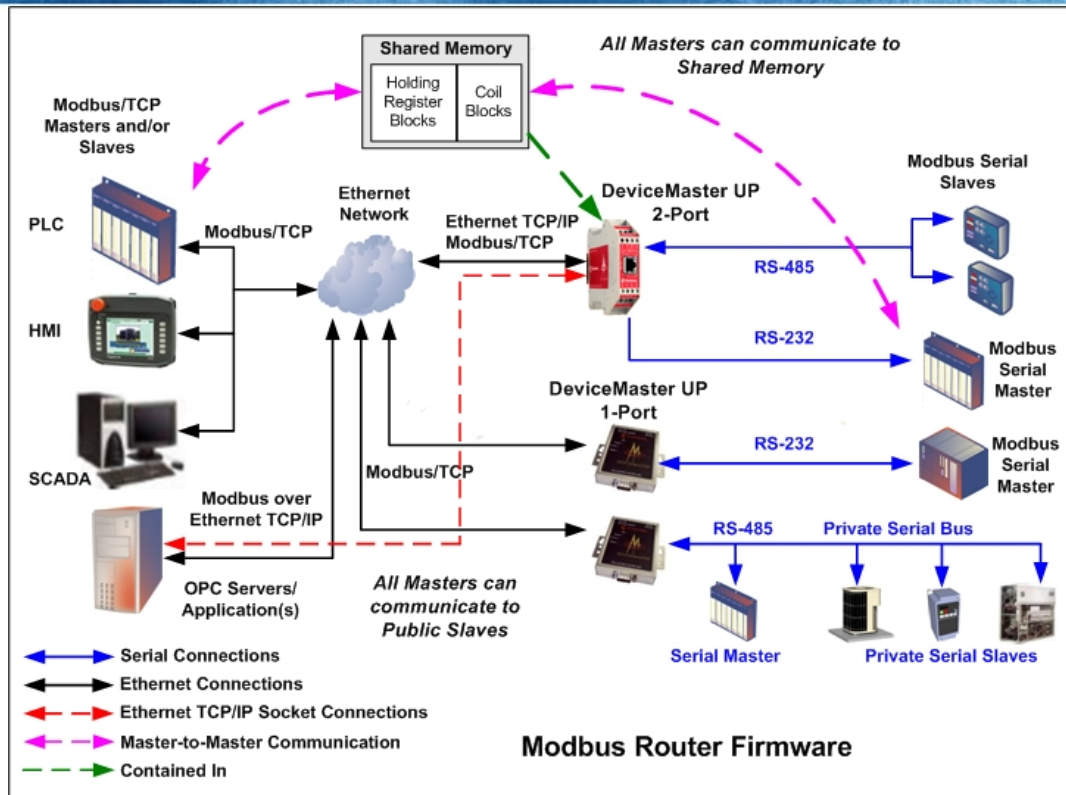
RSA® Conference 2018



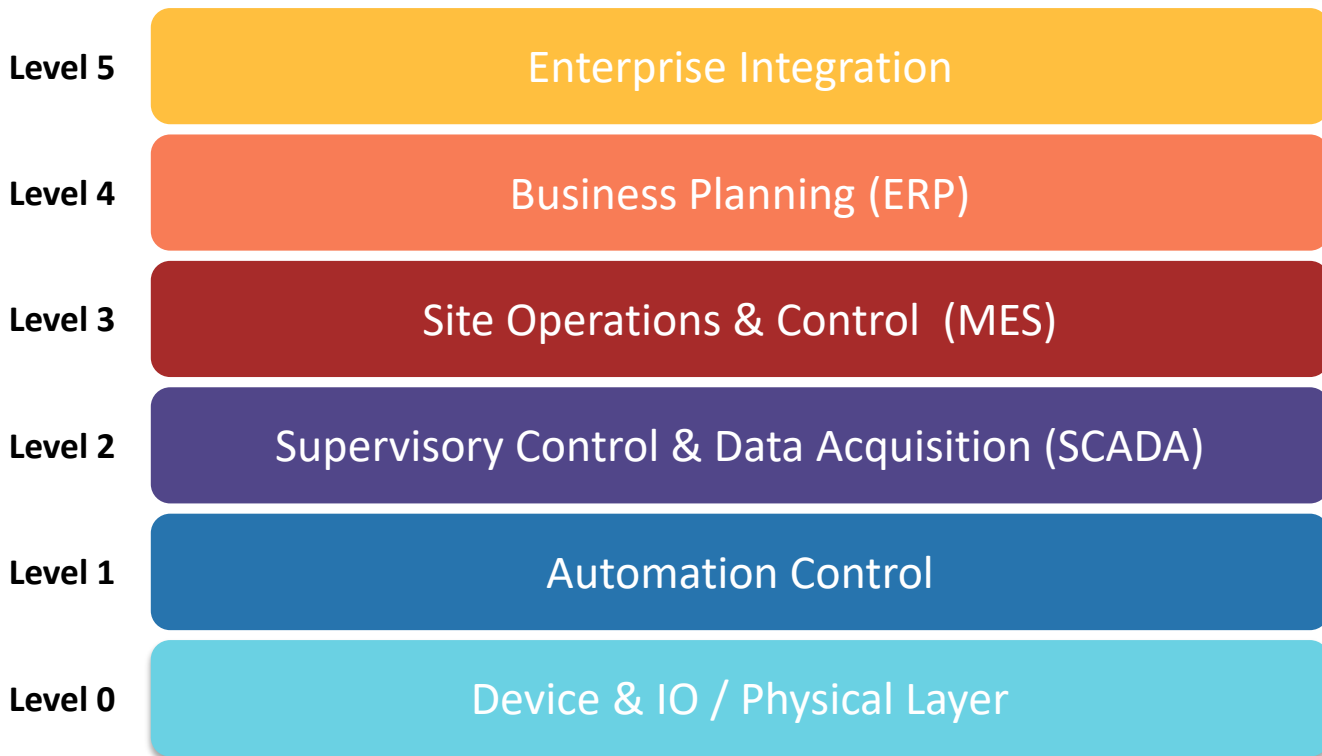
#RSAC

COMMUNICATION METHODOLOGY

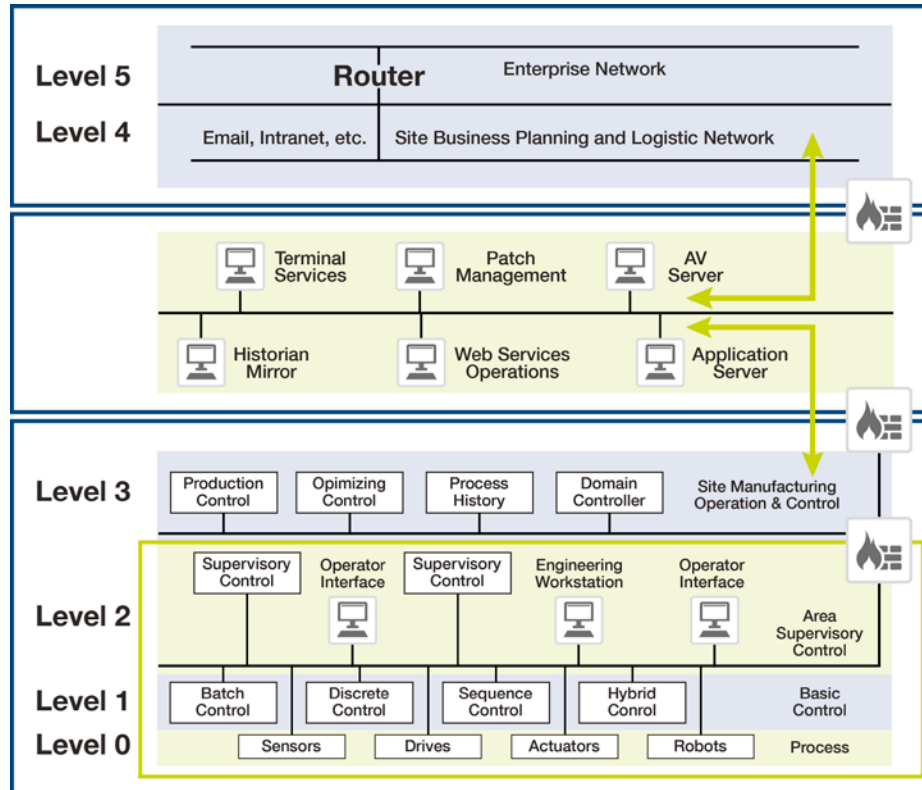
Communication Methods



The Purdue Model Simplified



The Purdue Model Detailed



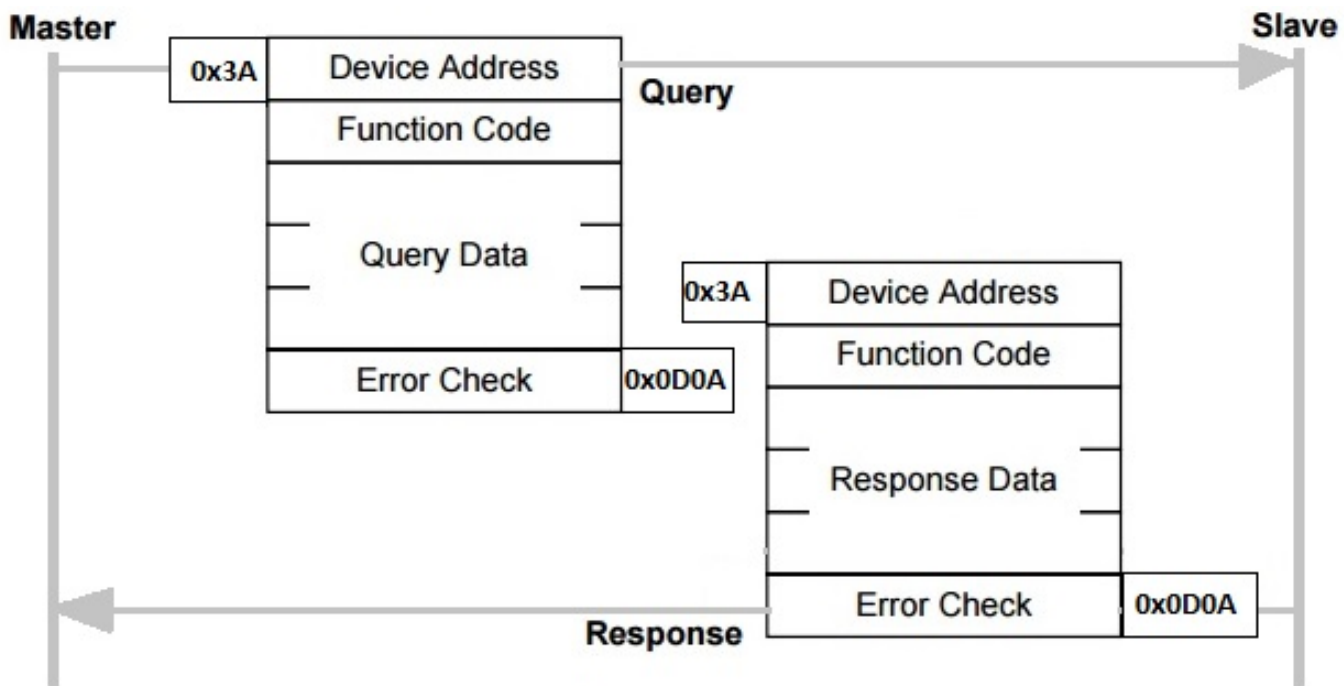
RSA® Conference 2018



#RSAC

INDUSTRIAL PROTOCOLS

MODBUS (MODIcon BUS)



Modbus Message Frames

CIP (Common Industrial Protocol)



Enter Settings Send the Request Set Response Data Types View the Results Log Results to a logfile

Simply Modbus TCP Client 8.0

mode: TCP IP Address: 192.168.100.100 Port: 502

Slave ID: 1 First Register: 40001 No. of Regs: 20

function code: 3 minus offset: 40001 register size: 16 bit registers

Request: 00 07 00 00 00 00 06 01 03 00 00 00 14

Response: 00 06 00 00 00 3B 01 03 28 55 6E 69 74 32 33 2D 41 FF FF 80 00 FF FF FF FA 80 00 00 00 43 7E E2 C6 42 0A C3 26 42 7D 7A EB 41 07 0E 38 00 00 00

copy down	register#	bytes	results	LOG	notes	clear notes
64b String8	40001	55 6E 69 74	Unit23-A		text label	
16bit UINT	40005	FFFF	65535		unsigned integer	
16bit INT	40006	8000	-32768		signed integer	
32bit UINT	40007	FFFF FFFA	4294967290		unsigned integer	
32bit INT	40009	8000 0000	-2147483648		signed integer	
32bit Float	40011	437E E2C6	254.88583		floating point value1	
32bit Float	40013	420A C326	34.69057		floating point value2	
32bit Float	40015	427D 7AEB	63.37004		floating point value3	
32bit Float	40017	4107 0E38	8.440971		floating point value4	
8bit UINT	40019	00	0		unsigned integer	
8bit UINT	40019	00	0		unsigned integer	
8 bits	40020	00	0000 0000		status 1-8	
8 bits	40020	07	0000 0111		status 9-16	

response time: 0.5 max: 0.6 avg: 0.525 min: 0.5

time between sends: 10.0 failed: 0

2015/10/02 13:58:30 >>> 00 06 00 00 00 06 01 03 00 00 00 14
 2015/10/02 13:58:30 <<< 00 06 00 00 00 3B 01 03 28 55 6E 69 74 32 33 2D 41 FF FF 80 00 FF FF FF FA 80 00 00 00 43 7E E2 C6 42 0A C3 26 42 7D 7A EB 41 07 0E 38 00 00 00 07

RSA® Conference 2018



#RSAC

LIVE HACK



- Modbus Set Point Injection
- CIP Replay Attack

RSA® Conference 2018

San Francisco | April 16 – 20 | Moscone Center



#RSAC

SESSION ID:

THANK YOU

Johnny Xmas

Security Researcher
Uptake
Johnny.Xmas@Uptake.com

Adam Ringwood

Security Researcher
Uptake
Adam.Ringwood@Uptake.com