Site SCADA (Purdue Levels 2-3)

Protocol Family	Serial Name	Physical Layer	# of Devices	Data Rate	Ethernet Name	EtherType	TCP/IP Name	TCP Port	UDP Port	Encryption
OPC	N/A				N/A		OPC DA	DCOM		
							OPC UA Binary	4840		TLS
							OPC UA XML	80, 443		TLS
Building Automation							BACnet/IP		47808	
							LonTalk		1628, 1629	
							Fox (Tridium/Niagara)	1911		
							KNXnet/IP	3671	3671	

Regional SCADA (Purdue Levels 2-3)

Protocol Family	Serial Name	Physical Layer	# of Devices	Data Rate	Ethernet Name	EtherType	TCP/IP Name	TCP Port	UDP Port	Encryption
Modbus	Modbus RTU	RS-232 TIA-485	247	9.6 Kbs - 12 Mbs	N/A		Modbus TCP	502	X	X
	Modbus ASCII	RS-232 TIA-485	65519				Modbus TLS	802	X	TLS
DNP	DNP3						DNP3 over TCP/IP	20000	20000	TLS
	WITS						WITS over TCP/IP	20000	20000	TLS
DLMS/COSEM (IEC 62056)	N/A						DLMS/COSEM	4059	4059	
IEC 60870	IEC 101						IEC 104	2404	2404	TLS
	N/A						ICCP/TASE2	102		
IEEE C37.118							IEEE C37.118	4712	4713	
IEC 61850					GOOSE	0x88B8	MMS	102		TLS
					GSSE	0x88B9				
					SV	0x88BA				
Time Synchronization	IRIG-A			1000 bps	PTP	0x88F7	NTP	X	123	
	IRIG-B			100 bps	N/A		PTP over UDP	X	319, 320	

Industrial Protocols Cheat Sheet v1.0

SANS ICS
ics.sans.org

By Don C. Weber & Justin Searle
don@cutawaysecurity.com |
justin@controlthings.io

This tri-fold cheat sheet provides details about common Industrial protocols that are be found in different areas of control networks. These protocols have been organized in the following sections:

- **Fieldbus and Fieldbus Management (Purdue Levels 0-1)**
- **Site SCADA (Purdue Levels 2-3)**
- **Regional SCADA (Purdue Levels 2-3)**

Details vary by protocol but include names, ethernet types, port numbers, and available encryption capabilities. For additional details about each protocol refer to the associated protocol specifications, vendor specifications, and other online documentation.

NOTE: Data provided in these tables have been taken from publicly available information to be used as a quick reference. Blank fields may mean that the information is not applicable or not available. Please contact the authors with any additional details about these and other protocols. Please provide supporting references. Applicable fields and corrections will be updated to future versions of this cheat sheet.

Fieldbus and Fieldbus Management (Purdue Levels 0-1)

Protocol Family	Serial Name	Physical Layer	# of Devices	Data Rate	Ethernet Name	EtherType	TCP/IP Name	TCP Port	UDP Port	Encryption
Modbus	(see Regional SCADA section)				N/A		(see Regional SCADA section)			
HART (Highway Addressable Remote Transducer)	HART		64	1.2 – 9.6 Kps			HART-IP	5094	5094	X
	Wireless HART	802.15.4	100+							
Foundation Fieldbus	FF H1	IEC 1158-2 ISA-S50.02	2 – 32	31.25 kbit/s	FF HSE		FF HSE	1089 - 1091	1089 - 1091	
	FF H2			1.0 Mbit/s 2.5 Mbit/s	N/A		N/A			
CIP (Common Industrial Protocol)	DeviceNET	Twisted Pair	64	125 kbit/s 250 kbit/s 500 kbit/s			EtherNet/IP	44818	2222, 44818	TLS or DTLS
	ControlNET	RG-6 Coaxial Cable	99	5 Mbit/s						
	CompoNET	TIA-485	384	93.75 kbps - 4 Mbps						
PROFINET	PROFIBUS DP		247	9.6 – 12 Mbit/s	PROFINET RT	0x8892	PROFINET	34962 - 34964	34962 - 34964	
	PROFIBUS PA	IEC 61158-2	32	31.25 kbit/s	PROFINET IRT					
FL-net					N/A		FL-net	55004	55000 - 55004	
P-NET (Process NETwork)	P-NET	TIA-485	32 – 125	76.8 kbit/s			N/A			
FIP (Factory Instrumentation Protocol)	WorldFIP		255	31.25kbit/s 1Mbit/s 2.5Mbit/s						
INTERBUS	INTERBUS									
CC-Link	Link	TIA-485	64	10 Mbit/s	Control	0x8800				
	LT				Field					
	Saftey	TIA-485		10 Mbit/s	Saftey					
Yokogawa Vnet	Vnet						Vnet/IP	5313	5313	
Toshiba TCnet	N/A				TCnet RTE	0x888b	TCnet			
EtherCAT					EtherCAT	0x88A4	EtherCAT UDP	X	34980	
Ethernet Powerlink					Ethernet Powerlink	0x88AB				
EPA (Ethernet for Plant Automation)					EPA	0x88BC	EPA			
Sercos (SErial Real-time Communication System)	Sercos I			2 Mbit/s 4 Mbit/s	Sercos III	0x88CD	N/A			
	Sercos II			2 Mbit/s 4 Mbit/s 8 Mbit/s 16 Mbit/s						
Yaskawa MECHATROLINK	MECHATROLINK-II	TIA-485	30	10 Mbit/s	MECHATROLINK-III					
CAN (Controller Area Network)	CANopen	CAN		10 kbit/s - 1 Mbit/s	N/A		DoIP	13400	13400	
	SAE J1939	CAN		250 kbit/s 500 kbit/s						
	SAE J2284	CAN		125 kbit/s 250 kbit/s 500 kbit/s						