ICS/OT Protocols			Communication Type						Topology					TC DP PA	U- Remote Terminal P-Transmission Cor -Decentralised Peri - Process Automatic	ntrol Protocol pherals	Dr. Yusuf Hashmi		
Protocol		Manufacturer	Serial	Ethernet	CAN Bus	RS 485 TCP/IP	Ring	Star	Bus	Р2Р	Linear Multi-	Master Multi-slave	Network		-Foundation H1 E-High Speed Ether Speed	Max Distance	Application		Constraints
Modbus	A simple, widely used protocol for industrial communication, available in both serial (RTU) and Ethemet (TCP) forms.	Schneider Electric	-	•	Н	H	Ŧ	Ŧ	Ŧ	—		-	-	RTU TCP	115.2 Kbps 10/100 Mbps	1200 m-RS485 N/W Dependent	SCADA systems, PLC communication	Simple, widely adopted, open protocol	RTU is slow, no native security
PROFIT®	An industrial Ethernet standard for automation that offers real-time capabilities and high-speed communication.	SIEMENS -		•			•	•		ļ.					100 Mbps -1 Gbps	100 m	Real-time control, Factory automation	High-speed, supports real-time communication	Requires managed switches, complex configuration
PROFO° MBOSM	A fieldbus communication standard used in automation, with variants for process automation (PA) and factory automation	SIEMENS	•			•		•	•					DP PA	Upto 12 Mbps 31.2 Kbps	1,200 m 1,200 m	Factory automation, process automation	High-speed, supports many devices	Higher latency compared to fieldbuses
CANOPER	A communication protocol based on CAN bus, often used in embedded systems and automotive applications.	CAN -			•							-		_	10 kbps to 1 Mbps	40 m at 1 Mbps, 6,000 m at 10 kbps	Embedded systems, vehicles, machinery	High reliability, good for noisy environments	Limited speed, distance trade-off
DeviceNet [®]	A network protocol used to connect industrial devices, based on CAN bus technology. Originally developed by Allen Bradley(Rockwell)	ODVA.			•				•				•		Up to 500 kbps	500 m	Industrial devices, sensor/actuator networks	High reliability, supports power and data on same cable	Limited speed and distance
EtherNet/IP*	A protocol that integrates standard Ethernet technology with industrial networking for real-time applications.	ODVA.		•			•	•		-				_	10 Mbps -1 Gbps	100 m per segment	Industrial networks, real-time control	Uses standard Ethemet, wide device support	DP is limited by cable length, PA is slow
COMMUNICATION PROTOCOL	A hybrid protocol that allows digital data to be transmitted over traditional 4-20 mA analog wiring.	FIELDCOMM GROUP* Connecting the World of Process Automation	•		- -				+	• •					1.2 kbps	1,500 m	Process automation, field instrumentation	Compatible with existing 4-20 mA systems	Limited speed, no real-time capabilities
AS(RAE) BACnet™	A digital, two-way communication system used in process control, supporting both H1 and HSE layers.	ASHRAE -		•	-		•	•	•						Up to 100 Mbps	100 m	Building automation systems, HVAC, lighting	Open protocol, multi- vendor interoperability	Ethemet version requires IT management
FOLKONTON	A digital, two-way communication system used in process control, supporting both H1 and HSE layers.	FIELDCOMM GROUP" Connecting the World of Process Automation	•						•					H1 HSE	31.25 kbps 100 Mbps	1,900 m 100 m	Process control, field devices	High reliability, supports complex networks	H1 is slow, requires specialized hardware
∠ ISi	A simple, cost-effective networking solution for connecting binary actuators and sensors in automation.	<u> </u>	•												Up to 167 kbps	100 m	Simple I/O devices, sensor/actuator networks	Simple installation, power and data on one cable	Limited to 31 devices per segment
EXPC UA	A platform-independent, service-oriented architecture that provides secure, reliable communication for industrial automation.	FOUNDATION											•)—	N/W Dependent	N/W Dependent	Industrial automation, IoT, cross-platform communication	High security, pltfrm independent, scala bility	High complexity, needs modetn architecture
dnp3	A protocol used primarily in utilities such as war electric, and gas industries for communication between control systems and remote devices.	er, % –	•	•					-	•	•		•		Up to 100 Mbps	N/W Dependent	SCADA systems, RTUs, substations	High reliability, supports time- stamped data	Complex to implement, limited to certain industries