Known SCADA ICS Network Ports

In a nutshell, Industrial control systems (ICS) are “computers” (PLC) that control the world around you. They’re responsible for managing the air conditioning in your office, the turbines at a power plant, the lighting at the theater or the robots at a factory. Most common SCADA systems with relative common use cases use the following network ports.

- BACnet (port 47808): is a communications protocol for building automation and control networks. It was designed to allow communication of building automation and control systems for applications such as heating, air-conditioning, lighting, and fire detection systems.
- Codesys: over 250 device manufacturers from different industrial sectors offer automation devices with a CODESYS programming interface. Consequently, thousands of users such as machine or plant builders around the world employ CODESYS for automation tasks.
- DNP3 (port 20000): Distributed Network Protocol is a set of communications protocols used between components in process automation systems. Its main use is in utilities such as electric and water companies.
- EtherNet/IP (port 44818): was introduced in 2001 and is an industrial Ethernet network solution available for manufacturing automation. General Electric (product:"general electric")
- GE Industrial Solution: Service Request Transport Protocol (GE-SRTP) protocol is developed by GE Intelligent Platforms (earlier GE Fanuc) for transfer of data from PLCs.
- HART IP: The HART Communications Protocol (Highway Addressable Remote Transducer Protocol) is an early implementation of Fieldbus, a digital industrial automation protocol. Its most notable advantage is that it can communicate over legacy wiring.
- IEC 60870–5–104
- IEC-104 (port 2404):is one of the IEC 60870 set of standards which define systems used for SCADA in electrical engineering and power system automation applications.
- Mitsubishi Electric (product:“Mitsubishi”): MELSEC-Q Series use a proprietary network protocol for communication. The devices are used by equipment and manufacturing facilities to provide high-speed, large volume data processing and machine control.
- Modbus (port 502): a popular protocol for industrial control systems (ICS). It provides easy, raw access to the control system without requiring any authentication.
- Omron: Factory Interface Network Service (FINS), is a network protocol used by Omron PLCs, over different physical networks like Ethernet, Controller Link, DeviceNet and RS-232C.
- PCWorx: is a protocol and program by Phoenix Contact used by a wide range of industries. We can find them by doing the following queries: port:20547,1962 PLC port:2455 operating system port:9600 response code
- ProConOS:a high-performance PLC run time engine designed for both embedded and PC based control applications.

- Red Lion (port 789 product:"Red Lion Controls"): Crimson v3.0 desktop software’s protocol used when communicating with the Red Lion Controls G306a human machine interface (HMI).
- Siemens S7 (port 102): S7 Communication, a proprietary protocol that runs between programmable logic controllers (PLCs) of the Siemens S7 family.
- Tridium Niagara Fox (ports 1911 and 4911): the Fox protocol, developed as part of the Niagara framework from Tridium, is most commonly seen in building automation systems (offices, libraries, Universities, etc.).
- BACnet/IP -- UDP/47808 Siemens S7 -- TCP/102 DNP3 -- TCP/20000, UDP/20000 EtherCAT -- UDP/34980 Ethernet/IP -- TCP/44818, UDP/2222, UDP/44818 FL-net -- UDP/55000 to 55003 Foundation Fieldbus HSE -- TCP/1089 to 1091, UDP/1089 to 1091 ICCP -- TCP/102 Modbus TCP -- TCP/502 OPC UA binary -- Vendor application specific OPC UA discovery server -- TCP/4840 OPC UA XML -- TCP/80, TCP/443 PROFINET -- TCP/34962 to 34964, UDP/34962 to 34964 ROC PLus -- TCP/UDP 4000 Red lion -- TCP/789 Niagara Fox -- TCP/1911, TCP/4911
- IEC-104 -- TCP/2404 Codesys -- Vendor application specific PCWorx -- TCP/20547, TCP/2455, TCP//9600
- ABB Ranger 2003: * TCP/10307, TCP/10311, TCP/10364 to 10365, TCP/10407, TCP/10409 to 10410, TCP/10412, * TCP/10414 to 10415, TCP/10428, TCP/10431 to 10432, TCP/10447, TCP/10449 to 10450, * TCP/12316, TCP/12645, TCP/12647 to 12648, TCP/13722, TCP/13724, TCP/13782 to 13783, * TCP/38589, TCP/38593, TCP/38600, TCP/38971, TCP/39129, TCP/39278
- Emerson / Fisher ROC Plus: * TCP/UDP/4000
- Foxboro/Invensys Foxboro DCSFoxApi * TCP/UDP/55555
- Foxboro/Invensys Foxboro DCS AIMAPI * TCP/UDP/45678
- Foxboro/Invensys Foxboro DCS Informix * TCP/UDP/1541
- Iconics Genesis32GenBroker (TCP): * TCP/18000
- Johnson Controls MetasysN1: * TCP/UDP/11001
- Johnson Controls MetasysBACNet: * UDP/47808
- OSIsoft PI Server: * TCP/5450
- Siemens Spectrum Power TG: * TCP/50001 to 50016, TCP/50018 to 50020, * UDP/50020 to 50021, TCP/50025 to 50028, * TCP/50110 to 50111
- SNC GENe * TCP/38000 to 38001, TCP/38011 to 38012, * TCP/38014 to 38015, TCP/38200, * TCP/38210, TCP/38301, TCP/38400, * TCP/38700, TCP/62900, TCP/62911, * TCP/62924, TCP/62930, TCP/62938, * TCP/62956 to 62957, TCP/62963, * TCP/62981 to 62982, TCP/62985, * TCP/62992, TCP/63012, TCP/63027 to 63036, * TCP/63041, TCP/63075, TCP/63079, * TCP/63082, TCP/63088, TCP/63094, TCP/65443
- Telvent OASyS DNA: * UDP/5050 to 5051, TCP/5052, TCP/5065, * TCP/12135 to 12137, TCP/56001 to 56099

OTR Context Group Formatted List:

You can copy and paste each line into your own Context Group on you OTR device.

80,102,443,502,530,593,789/tcp
1089-1091,1541,1911,1962,2404/tcp
2455,4000,4840,4911,5052,5450,5065,9600/tcp
10307,10311,10364,10365,10407/tcp

10409-10410,10412,10414-10415,10428/tcp
10431,10432,10447,10449,10450,11001,12135-12137,12316/tcp
12645,12647,12648,13722,13724,13782,13783/tcp
18000,20547,34962,34964/tcp
38000-38001,38011-38012/tcp
38014-38015,38200,38210,38301,38400,38700,/tcp
38589,38593,38600,38971,39129,39278/tcp
44818,45678,46824,47808,50001-50016/tcp
50018-50020,50025-50028/tcp
50110-50111,55555/tcp
56001-56099
62900,62911,62924/tcp
62930,62938,62956-62957,62963/tcp
62981-62982,62985,62992,63012/tcp
63027-63036,63041,63075,63079/tcp
63082,63088,63094,65443/tcp
1089-1091,1451,2222,4000,11001,20000/udp
34980,44818,45678,47808/udp
55000-55003,50020,50021,55555/udp
5050-5051/udp
