

Appendix B—Terms and Definitions

Many terms and definitions that are specific to the SCADA and control systems community may conflict with other industrial terms, definitions, acronyms, etc. The following glossary is meant to provide a useful reference of terms, definitions, and acronyms that are specific to this community. Please note that several of the glossary items listed may be indicative of other communities, such as information technology (IT) (e.g., “local area network” or “LAN” is IT-specific).*

AC Drive: Alternating current drive; synonymous with *Variable frequency drive (VFD)*.

Application server: A computer responsible for hosting applications to user workstations.

Backup domain controller: Backup to the *Primary domain controller*.

Control server: A server hosts the supervisory control system, typically a commercially available application for DCS or SCADA systems, and communicates data between the peer-to-peer network and the LAN.

Data: A repository of information that usually holds plant wide information including process data, recipes, personnel data, and financial data.

DC servo drive: A specific type of drive that works specifically with servo motors. Transmits commands to the motor and receives feedback from the servo motor’s resolver or encoder.

Distributed control system (DCS): A supervisory control system that typically controls and monitors set points to sub-controllers distributed geographically throughout a factory.

Distributed plant: A geographically distributed factory that is accessible through the Internet by an enterprise.

Domain controller: A Windows server responsible for managing domain and authentication information which includes login user names and passwords.

Enterprise: A business venture or company that encompasses one or more factories.

Enterprise resource planning (ERP) system: A system that integrates enterprise-wide information including human resources, financials, manufacturing, and distribution as well as connects the organization to its customers and suppliers.

* Some terms and definitions (along with our thanks) have been taken courtesy of a NIST whitepaper, *IT Security for Industrial Control Systems*, Authors: Joe Falco, Keith Stouffer, Albert Wavering, and Frederick Proctor, Intelligent Systems Division, National Institute of Standards and Technology (NIST); URL: <http://www.isd.mel.nist.gov/documents/falco/ITSecurityProcess.pdf>.

- Fieldbus:** A category of network that links sensors and other devices to a PC or PLC-based controller. Use of Fieldbus technologies eliminates the need of point-to-point wiring between the controller and each device. A protocol is used to define messages over the Fieldbus network with each message identifying a particular sensor on the network.
- Firewall:** A device on a communications network that can be programmed to filter information based on the information content, source, or destination.
- Human–machine interface (HMI):** The hardware or software through which an operator interacts with a controller. An HMI can range from a physical control panel with buttons and indicator lights to an industrial PC with a color graphics display running dedicated HMI software.
- Internet:** A system of linked networks that are worldwide in scope and facilitate data communication services. The Internet is currently a communications highway for millions of users.
- Input/output (I/O):** A module relaying information sent to the processor from connected devices (input) and to the connected devices from the processor (output).
- Light tower:** A device containing series of indicator lights and an embedded controller used to indicate the state of a process based on an input signal.
- Local area network (LAN):** A network of computers that span a relatively small space. Each computer on the network is called a node, has its own hardware, and runs its own programs, but can also access any other data or devices connected to the LAN. Printers, modems, and other devices can also be separate nodes on a LAN.
- Machine controller:** A control system/motion network that electronically synchronizes drives within a machine system instead of relying on synchronization via mechanical linkage.
- Modem:** A device that allows a computer to communicate through a phone line.
- Management information system (MIS):** A software system for accessing data from production resources and procedures required to collect, process, and distribute data for use in decision making.
- Manufacturing execution system (MES):** Systems that use network computing to automate production control and process automation. By downloading “recipes” and work schedules and uploading production results, an MES bridges the gap between business and plant-floor or process-control systems.
- OPC client/server:** A mechanism for providing interoperability between disparate field devices, automation/control, and business systems.
- Peer-to-peer network (P2P):** A networking configuration where there is no server, and computers connect with each other to share data. Each computer acts as both a client (information requestor) and a server (information provider).
- Photo eye:** A light-sensitive sensor utilizing photoelectric control that converts a light signal into an electrical signal ultimately producing a binary signal based on a interruption of a light beam.
- Pressure regulator:** A device used to control the pressure of a gas or liquid.
- Pressure sensor:** A sensor system that produces an electrical signal related to the pressure acting on it by its surrounding medium.

- Primary domain controller:** A Windows server responsible for managing domain and authentication information which includes login user names and passwords, and is the primary controller for security functions, usually paired with a secondary (or backup) domain controller (See *Backup domain controller*).
- Printer:** A device which converts digital data to human readable text on a paper medium.
- Process controller:** A proprietary, typically rack mounted, computer system that processes sensor input, executes control algorithms, and computes actuator outputs.
- Programmable logic controller (PLC):** A small industrial computer used in factories originally designed to replace relay logic of a process control system and has evolved into a controller having the functionality of a process controller.
- Proximity sensor:** A non-contact sensor with the ability to detect the presence of a target, within a specified range.
- Redundant control server:** A backup to the control server that maintains the current state of the control server at all times.
- Remote terminal unit (RTU):** A computer with radio interfacing used in remote situations where communications via wire is unavailable. It is usually used to communicate with remote field equipment. PLCs with radio communication capabilities are also used in place of RTUs.
- Servo valve:** An actuated valve whose position is controlled using a servo actuator.
- Sensor:** A device that senses or detects the value of a process variable and generates a signal related to the value. Additional transmitting hardware is required to convert the basic sensor signal to a standard transmission signal. Sensor is defined as the complete sensing and transmitting device.
- Single-loop controller:** A controller that controls a very small process or a critical process.
- Solenoid valve:** A valve actuated by an electric coil. A solenoid valve typically has two states: open and closed.
- Supervisory control and data acquisition (SCADA) system:** Similar to a *Distributed control system* with the exception of sub-control systems being geographically dispersed over large areas and accessed using *Remote terminal servers*.
- Temperature sensor:** A sensor system that produces an electrical signal related to its temperature and, as a consequence, senses the temperature of its surrounding medium.
- Variable frequency drive (VFD):** A type of drive that controls the speed, but not the precise position, of a non-servo, AC (alternating current) motor by varying the frequency of the electricity going to that motor. VFDs are typically used for applications where speed and power are important, but precise positioning is not.
- Workstation:** A computer used for tasks such as programming, engineering, and design; the computer may or may not be network-connected or may be isolated from any network (telephone- or Ethernet-based).

Wide area network (WAN): A network that spans than a LAN, consisting of two or more LANs connected to each other via telephone lines, other networked connections, or very large area networks, such as the Internet.

Wireless device: A device that connects an automation system via radio frequency (RF) or infrared (heat) waves, to collect and/or monitor data, but may also modify control set points of control systems.