Industrial Control Systems (ICS)

Proficiency Code: A

Be mindful there are many control systems currently used to control industrial process all around the world. These processes include many production activities such as food preparation, water treatment, and nuclear power. As a cyberspace support specialist, you are responsible to support defensive, offensive, and restoration operations. One of the many systems you will encounter is the Supervisory Control and Data Acquisition System (SCADA). SCADA refers to a centralized system that monitors and controls industrial sites or complexes of systems spread out over large areas. Most control actions are automatic by remote terminal units or by programmable logic controllers. Host control functions are usually restricted to basic overriding or supervisory level intervention. SCADA systems occur in ***industrial control systems*** such as computer systems that monitor and control industrial infrastructure. SCADA is data-acquisition oriented, event driven, expected to operate despite failure of field communications, and is preferred for applications that are spread over a wide geographic location. SCADA systems unlike distributed control systems (DCS), coordinates, but does not control processes in real-time. A SCADA system usually consists of:

- A human-machine interface or human machine interface (HMI) is the apparatus that presents process data to a human operator, and through this, the human operator monitors and controls the process.

- A supervisory (computer) system, gathers (acquires) data on the process and sends commands (control) to the process.

- Remote terminal units (RTU) connect to sensors in the process, converting sensor signals to digital data, and sending digital data to the supervisory system.

- Programmable logic controller (PLC) used as field devices because they are more economical, versatile, flexible, and configurable than special-purpose RTUs.

- Communication infrastructure connecting the supervisory system to the remote terminal units.

SCADA systems are typically implemented as a distributed database, commonly referred to as a *tag database*, which contains data elements called *tags* or *points*. A point represents a single input or output value monitored or controlled by the system. Points can be either “hard” or “soft.” A hard point represents an actual input or output within the system, while a soft point results from logic and math operations applied to other points.