- Filename: eccouncil-ceh31250-v11-18-4-1-ot-basics.md
- Show Name: CEHv11 (312-50)
- Topic Name: Mobile Platform, IoT, and OT Hacking - IoT and OT Hacking
- Episode Name: OT Basics
==

OT Basics

Objectives:

- What is OT

  - Operational Technology

    - Managing, Monitoring, and Controlling industrial operations

      - Focused on the physical devices and processes they use

- OT Components/Systems

  - ICS (Industrial Control System)
  - SCADA (Supervisory Control And Data Acquisition)

    - Gathers and presents data to operators
    - Make decisions about processes with the aid of operator input
    - Control plant functions based on those decisions

  - DCS (Distributed Control System)

    - Like SCADA, but focused more on automation

  - PLC (Programmable Logic Controller)
  - RTU (Remote Terminal Unit)

    - aka Remote Telemetry Unit and Remote Telecontrol Unit

      - A 'beefed-up' PLC

        - Better environmental tolerances
        - Backup power options
        - Autonomy

  - BPCS (Basic Process Control System)
  - SIS (Safety Instrumented Systems)

    - Sensors, logic solvers, and final control elements

      - Protects personnel, equipment, and environment

        - Isolates the plant in case of an emergency

  - HMI (Human Machine Interface)

    - Screen that allows a human to interact with a machine

      - Data input/output

        - Subset of SCADA

  - IED (Intelligent Electronic Devices)

    - Devices that receive data from sensors and/or power equipment

      - Issue control commands like

- Tripping breakers during voltage/current/frequency anomalies
  - Example device: voltage regulator
- IIOT (Industrial Internet of Things)
  - The convergence of OT and IT
    - Using traditional IT infrastructure to manage OT devices
- OT Security Challenges
  - Plain Text Passwords/Protocols
  - Complexity
  - Proprietary tech
  - Legacy Tech
  - Lack of security professionals
  - Converging with IT brings in IT Security issues