Emerging Threats – Device connectivity

- Vehicles

  - Vendor software updates, traffic lights and signs, traffic info, multimedia and active contents, Bluetooth, …

  - A car has 40-50 computers connected via a LAN

  - Protection does not include a firewall

- Process control systems

What is a Process Control System (PCS)?

- Standard off-the shelf components
  - Embedded computer systems

- Hardware and software that monitors and manages a process of interest
  - Supervisory control and data acquisition (SCADA)
  - Distributed control system (DCS)

- Components include
  - Human-machine interface (HMI)–monitors process
  - Historian–stores historical data
  - Measure/Control Unit
    - Programmable Logic Controller (PLC)
    - Remote Terminal Unit (RTU)

Human Machine Interface
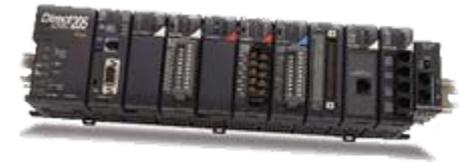
Programmable Logic Controller

Emerging Threats – Device connectivity

- Process control systems
  - Hardware and software has evolved to enable internet connections
  - Threat model has not changed!

- Example of use (US) –
  - 2M Miles of pipeline – *Gas to homes*
  - 80,000 dams and 1600 water treatment plans – *Water to homes*
  - 2800 power plants (104 nuclear) – *Electricity to homes*

- Failures of Process Control Systems are Serious Events

- Example Brisbane, AU:
  - Disgruntled former employee
  - Laptop and radio acting as "Pumping station #4" reprogrammed PCS
  - Sewage poured into a river and a residential area

- Company networks are better protected than these systems!

- Obvious targets for attacks / warfare