Linux Watchdog

* Watchdog Timer
  + Guards against systems locking up
  + Working software periodically “hits” the watchdog
  + If the watchdog times out, it restarts the board
* Applications
  + Most embedded systems use a watchdog to allow recovering from faults
  + Critical in applications where humans cannot reboot
* Usage
  + Opening /dev/watchdog starts timer
  + Writing anything to it resets timeout, if it expires, the board resets
  + If the program exits, the watchdog needs to be explicitly crashed, otherwise it keeps running to detect application crashes

FMEA

* Developers often focus on new features, not full systems in use
  + Writing a project that has no ways to add users to user database because there is no API
* How component failures in a complex system affect its overall performance
  + Shows us how the system is likely to fail in the field
* Failure Mode and Effect Analysis
  + Brainstorm how components of a system can fail
  + Rate what the effect of the failure is, how likely, and how to detect the failure
  + Compute what the risk is for this possible failure
* Steps:

1. Imagine how some component could fail
2. List effects of failure
   1. Rate severity (1-10)
3. Think what could cause the failure
   1. Rate likelihood (1-10)
4. State how this failure is currently detected
   1. Rate detected effectiveness (1-10)
5. Compute Risk Priority Number [RPN]
   1. Multiply above three scores (1-1000)
6. List possible actions to reduce this risk

Complex Systems

* Challenges with hardware
  + Takes months to build
  + Time consuming to test
* Effective Testing
  + Mock hardware: Hardware Abstraction Layer (HAL) in software
  + Bench testing
  + Real hardware
* Danger Zone
  + Linear System: breakdown at stage N is immediately obvious at stage N+1
  + Complex System: hidden interactions
    - Poor visibility
    - Indirect measurements
    - In event of a failure, it is unclear where the issue originated
  + Coupling
    - Tightly coupled – no opportunity to redo a task or correct a failure
    - Loosely coupled – a problem can be worked around
  + Graph complex vs coupling
    - Simple to complex
    - Loose to tight coupling
    - Complex and tightly coupled systems are located in the “danger zone”