When Embedded Systems Attack...

- Embedded systems can fail for a variety of reasons
  - Electrical problems
  - Mechanical problems
  - Errors in the programming
  - Incorrectly specified
  - Errors caused by users
  - Zillion other reasons
- Some failures have been well documented and can be used to learn how to make systems better.

Therac-25

- The Therac-25 was a medical radiation therapy machine developed in the mid-1980s.
- Controlled by a PDP-11 (16-bit minicomputer)
- Errors in the hardware/software design let to three patients being killed and many injured.

Therac-25

- Examination of the system revealed numerous defects that could lead to improper operation:
  - Insufficient hardware/software interlocks to prevent dangerous types of actions.
  - Certain unusual patterns of keystrokes could put the system in the incorrect mode.
  - Software was reused from previous models despite changes in the overall design.
  - No way for software to tell if the hardware was doing what it was told to do (open loop control).
  - Control tasks and operator tasks were not synchronized leading to possible race condition.
  - Overflows in some variables were not detected.

Mars "Spirit" Rover

- Suffered a severe “anomaly” upon landing that nearly aborted the mission.
Mars "Spirit" Rover

- Spirit appeared to be working as expected after landing, but soon started having problems.
- JPL could contact it to give it commands and know that it was alive but very little data was being received.
- Eventually concluded that the rover was resetting continuously due to problems with the software stored in FLASH memory.
- Spirit was commanded to run in “crippled” mode where it doesn’t use the FLASH data.
- JPL had control of it, sort of, but what was wrong?

- For 11 Martian days, the JPL team worked to diagnose and fix the problem.
- Data in the FLASH memory was believed to be corrupted.
- Eventually reformatted the FLASH and loaded new data.
- Problem caused by way the OS used memory to implement a file system in the FLASH.
- Processes could run out of available memory and get stuck causing a reset.
- Eventually fixed and returned to full operation.

Toyota Unintended Acceleration

- Over the last 6+ years many claims that Toyota vehicles were subject to sudden unintended acceleration problems.
- Vehicle throttles use “drive-by-wire” system
  - No mechanical connection between the throttle pedal and the engine.
  - Computers sense the position of the throttle and adjust the engine power accordingly.
  - Similar to “fly-by-wire” system in use in current military and commercial aircraft and in the space shuttle.
- Toyota and NHTSA claimed the problem was with floor mats or drivers pressing the throttle instead of the brake.
- Eventually resulted in numerous lawsuits
- Testimony by expert witnesses for the plaintiffs have pointed to numerous potential problems in the embedded systems running the vehicles.
  - Disclaimer: Testimony is not proof, just an opinion.
• Some possible problems were identified during litigation:
  – Possible for a single bit flipped to cause the problem.
  – Portions of the memory were not protected against corruption due to stack overflows and software bugs.
  – One task was handling numerous functions including failsafes and brake override.
  – Tasks could terminate without the OS noticing.
• Vehicle software is not designed to the same standards as required by law in aircraft, medical devices, etc.

• Do we have unreasonably high expectation for the reliability of consumer electronic devices?
• How much are people willing to pay for reliability?
  – “Fly by wire is done on aircraft -- and if you have flown on a 757,767,747-400,787,777, or any Airbus Airliner, you have depended on this technology from take-off to landing -- The best of these systems are Quadruple Redundant (typically three redundant actuators and dual sticks, plus redundant trim switch controls -- plus a dissimilar backup system -- in these systems the power systems are triple redundant or quadruple redundant as well.” - EETimes.com blogger
• How much would a car cost if you demanded the same reliability and redundancy as in an aircraft?