Embedded System Design and Synthesis

Robert Dick

http://robertdick.org/esds/
Office: EECS 2417-E
Department of Electrical Engineering and Computer Science
University of Michigan




Example medical devices

?

Special characteristics

- Real-time.
- Extreme consequences for failures.
- Coupled physical, computation systems, which may be complex.
- Subject to use by experts in other areas who are naïve about the technology employed.
- Require high rate signal processing and decision making.
- Tight power consumption constraints.
- Regulatory process stressing informal testing techniques.

Therac-25

- AECL Medical (Medical device company owned by Canadian government).
- Designed from start for software control using PDP 11.
  - Hardware interlocks eliminated, relied on software.
- Custom real-time executive.
  - No explicit synchronization.
  - Non-atomic test and set.
  - Shared memory.
    - What about HP guidelines.
- User interface making failure difficult to detect, and encouraging ignoring warnings.

Malfunction 54

- Common cryptic error messages, most of which did not indicate danger to patients.
- Operators learned to ignore warnings.
- Operators taught that there are "so many safety mechanisms" that it is virtually impossible to harm a patient.
  - Milgram + Monderman.

Consequences and responses

- Holes burned in people.
- Paralyzed arm, legs, vocal cords, and lung, followed by death.
- Destroyed brain.
- Victims were told by technicians that this is "impossible", at least until their skin fell off.
- Blamed on mechanical errors, additional checks applied, deemed "corrected".

Causes?

- System checked for edits only if bending magnet flag is set.
- Edits made within 8 seconds, while bending magnets were being adjusted, not detected.
- Real causes?
- "We know there are many safety codes, guides, and regulations to guide them." Rawlinson
- Human tendency to see patterns where none exist.
- Unrealistic risk assessments.

Testing vs. formal verification

- Precise specification.
- Efficient state space representation.
- Symbolic checking.

Homework

- Due 27 October: Ben W. Cook, Steven Lanzisera, and Kristofer S. J. Pister. SoC issues for RF smart dust. *Proc. IEEE*, 94(6), June 2006.
- Due 1 November: Joo-Young Hwang, Sang-Bum Suh, Sung-Kwan Heo, Chan-Ju Park, Jae-Min Ryu, Seong-Yeol Park, and Chul-Ryun Kim. Xen on ARM: System virtualization using Xen hypervisor for ARM-based secure mobile phones. In *Proc. Consumer Communications and Networking Conf.*, pages 257–261, January 2008.
- Due 1 November: Srivaths Ravi, Anand Raghunathan, Paul Kocher, and Sunil Hattangady. Security in embedded systems: Design challenges. *ACM Trans. Embedded Computing Systems*, August 2004.