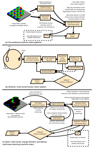
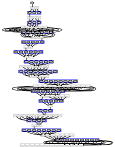
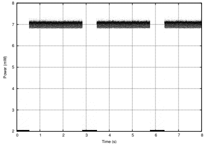
Introduction to Embedded Systems Research: Notes on Reliability

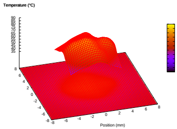
Robert Dick

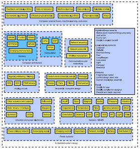
dickrp@umich.edu
Department of Electrical Engineering and Computer Science
University of Michigan


(a) Conventional machine vision pipeline
(b) Iterative, multi-round human vision system
(c) Goal: multi-round, energy-efficient, low-latency continuous-learning machine vision









Outline

1. Deadlines and announcements
2. Reliability
3. IoT reliability

Deadlines and announcements

25 Oct.: Midterm exam.

8 Nov.: Second (and last) project checkpoint.

Early December: Project presentations.

9 Dec.: Project deadline.

8am–10am 15 Dec.: Final exam.

Outline

1. Deadlines and announcements
2. Reliability
3. IoT reliability

Testing

64-bit adder → 2^{128} input vectors.

Coverage is imperfect.

Control inputs.

Observability via outputs / probe points.

Single stuck-at fault model.

Scan chain.

Formal Methods and Model Checking

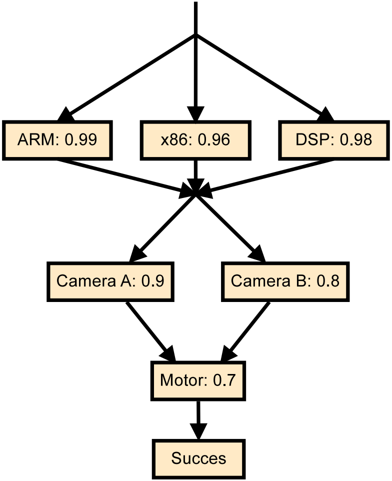
Requires formal specification and property descriptions.

Exhaustively prove that certain properties hold for all input vectors.

Theorem providing, SAT solving, etc.

Computatuonally expensive.

Reliability modeling



Arbitrary reliability calculations

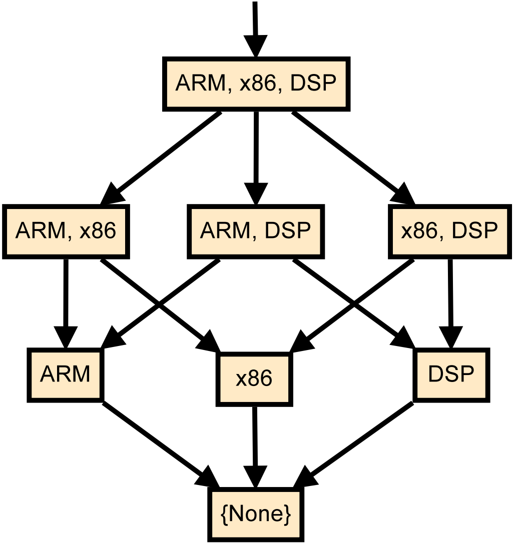
ARM 0.99	x86 0.96	DSP 0.98	Stage success	Probability
0	0	0	0	$0.01 \cdot 0.04 \cdot 0.02 = 8 \times 10^{-6}$
0	0	1	1	$0.01 \cdot 0.04 \cdot 0.98 = 0.00039$
0	1	0	1	$0.01 \cdot 0.96 \cdot 0.02 = 0.00019$
0	1	1	1	$0.01 \cdot 0.96 \cdot 0.98 = 0.0094$
1	0	0	1	$0.99 \cdot 0.04 \cdot 0.02 = 0.00079$
1	0	1	1	$0.99 \cdot 0.04 \cdot 0.98 = 0.039$
1	1	0	1	$0.99 \cdot 0.96 \cdot 0.02 = 0.019$
1	1	1	1	$0.99 \cdot 0.96 \cdot 0.98 = 0.93$

Shortcuts for parallel and series

Parallel: $P_{succeed,sys} = 1 - \prod_{i \in N} (1 - P_{succeed,i})$.

Series: $P_{succeed,sys} = \prod_{i \in N} P_{succeed,i}$.

Fault tree



Fault tree exploration

Fault tree size in number of components?

Exhaustive exploration often computationally intractable.

Monte Carlo variants.

Outline

1. Deadlines and announcements
2. Reliability
3. IoT reliability

Statistical modeling impractical

Assumption: statistical independence.

Usually wrong.

For security, very wrong.

Deceptive for IoT reliability estimation.

Implicit correlations through environment and social effects, etc.

How can the problem be solved?

IoT security/reliability problem more akin to social/financial catastrophe prediction than isolated embedded system analysis.

Stamp collecting vs. science of design.

How can the situation be improved?

Incentive structures?

Ronen et al.

Single-company design: entire design known.

Model checking not used.

Implementation error in use of proximity detection.

Use of symmetric key with utterly unrealistic assumption about leak probability.

IoT will grow into something much harder to secure.

No formal design specification for entire system

Designed by many companies that won't share specs or implementations.

Formal models and model checking impractical.

Any attempt at model checking requires arbitrary number of components with unknown possible states.

Probably infeasible to specify.

State space explosion.

Highly (uselessly) conservative.

Large-scale with heterogeneous components

Sensors.

Actuators.

Computers.

Transceivers.

All broaden the attack surface.