Professional Considerations in Digital System Design

RELIABILITY AND SAFETY ANALYSIS

David G Meyer ©2020, Images Property of their Respective Owners
• Introduction
• Component Failures and Wear
• Definition of Failure Rate
• Reliability Models for Components
• Mean Time To/Before Failure (MTTF/MTBF)
• Failure Mode & Effects Analysis (FMEA)
• Criticality Analysis (FMECA)
• Revisiting the Nest Case Study
• Software Reliability
• Maintainability
• Standards and Compliance

INTRODUCTION

- Reliability, maintainability, and safety integral to product development
- Tradeoffs between requirements and cost
- Reducing probability of failure is expensive
- Given little potential for personal injury, the primary consideration is manufacturing cost vs. potential customer unhappiness
- There are UL, CE, IEC, FCC standards (possibly others) to be met
COMPONENT FAILURES AND WEAR

- Electronic components can most often be modeled by constant failure rate ($\lambda$)*
- Leads to exponential failure distribution
- Same probability of failure in the next hour regardless of whether it is new or used – result is a “bathtub curve”

*but...see also May 2011 IEEE Spectrum feature article on “Transistor Aging”
• Components do not “age” or “degrade” with use – constant failure rate unrelated to hours of use (*under certain conditions*)

• Equivalent information is gained testing 10 units for 10,000 hours vs. testing 1000 units for 100 hours

• “Impossible” 10⁻⁹ failure as likely to happen in the first five minutes of operation as 114,000 years from now

• Infant mortality reduced by robust designs, manufacturing process control, and “shake and bake”
DEFINITION OF FAILURE RATE

• Units: usually given in terms of failures per hour, normalized for a single unit

• Not really a probability, but rather an “expected value”

• More intuitive way to describe: “unit failures per million hours per unit”, i.e. \[\frac{\text{fails}}{\left(10^6 \text{ hour} \times \text{unit}\right)}\]

• Equivalent to:
  • number of failures per unit per million hours
  • number of failures/hour given one million units in field (assuming failed units are replaced)
DEFINITION OF FAILURE RATE

• Given $\lambda_p \times 10^{-6}$ [fails/(hr x unit)], N [units] in the field and T [hours]
  • expected number of failures in T hours
    ➢ $F$ (no. of failures) = $\lambda_p \times 10^{-6}$ fails/(hr x unit) $\times$ N units $\times$ T hours
    ➢ $F = \lambda_p \times 10^{-6} \times N \times T$ failures (all other units cancel out)
• example: given 1000 units in the field (at all times), and $\lambda_p = 2 \times 10^{-6}$, how many failures would you expect in one year?
  ➢ $F = 2 \times 10^{-6}$ fails/(hr x unit) $\times$ 1000 units $\times$ (365 $\times$ 24) hours = 17.52
DEFINITION OF FAILURE RATE

- Given $\lambda_p \times 10^{-6}$ [fails/(hr $\times$ unit)], $N$ [units] in the field and $T$ [hours]
  - expected number of failures in $T$ hours
    - $F$ (no. of failures) = $\lambda_p \times 10^{-6}$ fails/(hr $\times$ unit) $\times$ $N$ units $\times$ $T$ hours
    - $F = \lambda_p \times 10^{-6} \times N \times T$ failures (all other units cancel out)

- suppose you are aiming for no more than one unit failure per week with 10,000 units in the field – what is an acceptable failure rate?
  - $F = \lambda_p \times 10^{-6} \times N \times T$ failures
  - $\lambda_p \times 10^{-6} = F/(N \times T) = 1$ failure / (10,000 $\times$ 7 $\times$ 24 hrs) = 0.595$\times$10$^{-6}$ failures per unit per hour
1. How long is $10^6$ hours?
   A. 41,667 days
   B. 1370 months
   C. 114 years
   D. all of the above
   E. none of the above
1. How long is $10^6$ hours?
   A. 41,667 days
   B. 1370 months
   C. 114 years
   D. all of the above
   E. none of the above

2. Given a failure rate of $1 \times 10^{-6}$ units/hour, should you be “happy*” if a typical single unit only fails once in 114 years on average?
   A. yes
   B. no
   C. (need more information)

* What regulations or standards should determine your degree of “happiness”?
3. How long between unit failures will it be if you have one million units in use?
   A. 0.1 hour (6 minutes)
   B. 1 hour
   C. 10 hours
   D. 1,000 hours
   E. 1,000,000 hours
3. How long between unit failures will it be if you have one million units in use?
   A. 0.1 hour (6 minutes)
   B. 1 hour
   C. 10 hours
   D. 1,000 hours
   E. 1,000,000 hours

4. Is this rate acceptable* if said failure causes serious injury or property damage?
   A. yes
   B. no
COMPONENT WEAR

• If, based on observation, failure rate does depend on time used, it may be due to wear caused by improper derating
• See also “An Odometer for CPUs,” IEEE Spectrum, May 2011
• Well-derated electronic systems seldom reach the point of wear-out failure
  • Well-derated = working at < 30-40% of specified ratings
  • Heat is the main reliability killer – even a small reduction will have a significant effect
  • Components like electrolytic capacitors can “dry out” and deteriorate over time (and/or become “leaky”)

PURDUE UNIVERSITY
COMPONENT WEAR

- Heat is the main reliability killer – even a small reduction will have a significant effect.
- Components like electrolytic capacitors can “dry out” and deteriorate over time (and/or become “leaky”).

Leaked electrolyte is highly corrosive!
Electrolytic capacitors used in switch-mode power supplies of this type must be “high temperature” (105°C) class.
Calculated value is $\lambda_p$, the predicted number of failures per $10^6$ hours of operation.

Examples (MIL-HDBK-217F):

**Diodes**

$\lambda_p = \lambda_b \times \pi_t \times \pi_T \times \pi_S \times \pi_C \times \pi_Q \times \pi_E$

where:

$\lambda_b$ = base failure probability related to the construction; 0.0012 for switching and general-purpose diodes, 0.0030 for power rectifiers, and 0.0013 for transzorbs.

$\pi_t$ = temperature coefficient; 3.9 for junction temperature $T_j < 70^\circ$C.

$\pi_S$ = is based on stress 1.0 for transzorbs and 0.054 for other diodes in the system, provided they are not exposed to more than 30% of their rated characteristics.

$\pi_C$ = contact construction factor; 1.

$\pi_Q$ = 8.0 for plastic encapsulated devices.

$\pi_E$ = environmental constant; 6.0 for the “ground fixed” environment.

A “ground fixed” environment is one with an average temperature of 25° C (not exceeding 45° C)

**Microelectronic Circuits**

$\lambda_p = \left( C_1 \times \pi_T + C_2 \times \pi_E \right) \times \pi_Q \times \pi_L$

where:

$C_1$ = die complexity; 0.14 for the PIC controller and 0.020 for the regulator 7805.

$\pi_T$ = temperature coefficient. Assuming the junction temperature $T_j < 100^\circ$C for both ICs, it will be 1.5 for the PIC controller and 16 for the regulator.

$C_2$ = a constant based on the number of pins. 0.0034 is used for the PIC with 8 pins and 0.0012 for the 3-pin regulator.

$\pi_E$ = environmental constant. Assume the equipment will operate in a “ground fixed” environment, a benign location with average ambient temperature of 25°C, not exceeding 45°C.

$\pi_L$ = learning factor; 1 for ICs more than two years in production.

$\pi_Q$ = quality factor. This is the most controversial coefficient. For military screened components it is between 1 and 2, but climbs to 10 for commercial components. Many critics have established that the penalty for commercial, off-the-shelf parts is unrealistically high, especially when taking into account modern manufacturing processes.
## RELIABILITY MODELS FOR COMPONENTS

### PN Junction Diode (Power Rectifier Application)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Value</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\lambda_D$</td>
<td>Diode type/application</td>
<td>0.0030</td>
<td>Power rectifier</td>
</tr>
<tr>
<td>$\pi_T$</td>
<td>Temperature factor</td>
<td>1.0</td>
<td>$T_J = 25^\circ C$</td>
</tr>
<tr>
<td>$\pi_S$</td>
<td>Electrical stress factor</td>
<td>0.29</td>
<td>$0.4 &lt; V_S \leq 0.5$</td>
</tr>
<tr>
<td>$\pi_C$</td>
<td>Contact construction</td>
<td>1.0</td>
<td>Metallurgically bonded</td>
</tr>
<tr>
<td>$\pi_Q$</td>
<td>Quality factor</td>
<td>8.0</td>
<td>Plastic case</td>
</tr>
<tr>
<td>$\pi_E$</td>
<td>Environmental factor</td>
<td>1.0</td>
<td>$G_B$</td>
</tr>
</tbody>
</table>

$$\lambda_p = \lambda_D \times \pi_T \times \pi_S \times \pi_C \times \pi_Q \times \pi_E = 6.96 \times 10^{-8}$$

# Reliability Models for Components

## Silicon MOSFET (Power Switching Application)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Value</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\lambda_b$</td>
<td>Base failure rate</td>
<td>0.012</td>
<td>MOSFET</td>
</tr>
<tr>
<td>$\pi_T$</td>
<td>Temperature factor</td>
<td>1.0</td>
<td>$T_J = 25^\circ C$</td>
</tr>
<tr>
<td>$\pi_A$</td>
<td>Application factor</td>
<td>2.0</td>
<td>Power FET</td>
</tr>
<tr>
<td>$\pi_Q$</td>
<td>Quality factor</td>
<td>8.0</td>
<td>Plastic case</td>
</tr>
<tr>
<td>$\pi_E$</td>
<td>Environmental factor</td>
<td>1.0</td>
<td>$G_B$</td>
</tr>
</tbody>
</table>

$$\lambda_p = \lambda_b \times \pi_T \times \pi_A \times \pi_Q \times \pi_E = 1.92 \times 10^{-7}$$

## RELIABILITY MODELS FOR COMPONENTS

### CMOS Switch-Mode Regulator IC (8 pin)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Value</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>$C_1$</td>
<td>Number of transistors</td>
<td>0.040</td>
<td>$300 &lt; x &lt; 1000$</td>
</tr>
<tr>
<td>$\pi_T$</td>
<td>Temperature factor</td>
<td>0.1</td>
<td>CMOS, $T_j = 25^\circ C$</td>
</tr>
<tr>
<td>$C_2$</td>
<td>Package failure rate</td>
<td>.0013</td>
<td>8-pin flatpack</td>
</tr>
<tr>
<td>$\pi_E$</td>
<td>Environmental factor</td>
<td>0.5</td>
<td>$G_B$</td>
</tr>
<tr>
<td>$\pi_Q$</td>
<td>Quality factor</td>
<td>2.0</td>
<td>Class B-1</td>
</tr>
<tr>
<td>$\pi_L$</td>
<td>Learning factor</td>
<td>1.0</td>
<td>$\geq 2 \text{ years}$</td>
</tr>
</tbody>
</table>

\[
\lambda_p = (C_1 \times \pi_T + C_2 \times \pi_E) \times \pi_Q \times \pi_L = 9.3 \times 10^{-8}
\]

## RELIABILITY MODELS FOR COMPONENTS

### CMOS 16-bit Microcontroller (TI MSP430, 80-pin QFP)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Value</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>$C_1$</td>
<td>Die complexity</td>
<td>0.28</td>
<td>16-bit CMOS</td>
</tr>
<tr>
<td>$\pi_T$</td>
<td>Temperature factor</td>
<td>0.1</td>
<td>CMOS, $T_J = 25^\circ C$</td>
</tr>
<tr>
<td>$C_2$</td>
<td>Package failure rate</td>
<td>.08724</td>
<td>80-pin flatpack</td>
</tr>
<tr>
<td>$\pi_E$</td>
<td>Environmental factor</td>
<td>0.5</td>
<td>$G_B$</td>
</tr>
<tr>
<td>$\pi_Q$</td>
<td>Quality factor</td>
<td>2.0</td>
<td>Class B-1</td>
</tr>
<tr>
<td>$\pi_L$</td>
<td>Learning factor</td>
<td>1.0</td>
<td>$\geq 2$ years</td>
</tr>
</tbody>
</table>

$\lambda_p = (C_1 \times \pi_T + C_2 \times \pi_E) \times \pi_Q \times \pi_L = 1.4324 \times 10^{-7}$

* $C_2 = 3 \times 10^{-5} \times (\text{no. pins})^{1.82}$

When properly derated, electronic components can most often be modeled by:

A. an exponential failure rate
B. a quadratic failure rate
C. a constant failure rate
D. a linear failure rate
E. none of the above
The failure rate $\lambda p$ is equivalent to:

A. unit failures per million hours per unit
B. the number of failures per unit per million hours
C. the number of failures/hour given one million units in the field (assuming failed units are replaced)
D. all of the above
E. none of the above
Assuming that all electronic components in a design are sufficiently de-rated, equivalent information can be gained by testing 10 units for 10,000 hours as by:

A. testing 100 units for 1000 hours
B. testing 1000 units for 100 hours
C. testing 10,000 units for 10 hours
D. all of the above
E. none of the above
Assuming your design goal is no more than *one unit failure per week* with 10,000 units in the field, an acceptable failure rate ($\lambda\cdot p$) would be approximately:

A. $1 \times 10^{-4}$
B. $1 \times 10^{-6}$
C. $6 \times 10^{-7}$
D. $6 \times 10^{-10}$
E. none of the above
MTTF/MTBF

• For irreparable parts, use mean time to failure (MTTF) = $1/\lambda$ for components with an exponential life distribution
• For assemblies with repairable parts, mean time between failure (MTBF) is appropriate
• Field returns are always a more powerful statement of performance than statistical predictions
• Reliability models are conservative - equipment generally outperforms the statistics (well designed equipment)
The following sections illustrate an example of reliability analysis:

- **Reliability Analysis**
  - Choose 3-5 components in your design that are most likely to fail (voltage regulators, power MOSFETs, etc. – basically anything operating above room temperature). The microcontroller and any other similarly high complexity ICs should be included. Such devices are not always the hottest on your board, they are usually the most complicated and have the most I/O pins. Be sure to briefly explain the reasons for your selections.
  - Perform calculations to determine the number of failures per $10^6$ hours and mean time to failure (MTTF) for each component, making any reasonable assumptions where necessary. State the model used and any assumptions you had to make. For each component you analyzed, present the parameters you used and the results obtained in a tabular format like the following:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Value</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>$C_1$</td>
<td>Die complexity</td>
<td>0.28</td>
<td>16-bit CMOS</td>
</tr>
<tr>
<td>$\pi_T$</td>
<td>Temperature factor</td>
<td>0.1</td>
<td>CMOS, $T_J = 25^\circ C$</td>
</tr>
<tr>
<td>$C_2$</td>
<td>Package failure rate</td>
<td>.08724*</td>
<td>80-pin flatpack</td>
</tr>
<tr>
<td>$\pi_E$</td>
<td>Environmental factor</td>
<td>0.5</td>
<td>$G_B$</td>
</tr>
<tr>
<td>$\pi_Q$</td>
<td>Quality factor</td>
<td>2.0</td>
<td>Class B-1</td>
</tr>
<tr>
<td>$\pi_L$</td>
<td>Learning factor</td>
<td>1.0</td>
<td>$\geq 2$ years</td>
</tr>
</tbody>
</table>

- **Comments regarding choice of parameter value, especially if you had to make assumptions**

- Summarize conclusions about the reliability of these components and/or the circuit in general. Suggest design or analysis refinements that would realistically improve the reliability of the design.
• **Failure Mode Effects Analysis**
• Bottom-up review of a system
• Examine components for failure modes
• Note how failures propagate through system
• Study effects on system behavior
• Leads to design review and possibly changes to eliminate weaknesses
• Addition of criticality analysis
• Not necessary to examine every component
  ➢ multiple components may have same failure effect
• Rearrange design into functional blocks
  ➢ consider component failures within those blocks that may be critical
• Create chart listing possible failures
  ➢ block, failure mode, possible cause, failure effects, method of detection, criticality, and probability*

* probability calculation not required for homework
FAILURE CAUSE/MODE/EFFECT/CRITICALITY

(USE CIRCUIT CELLAR REFERENCE ARTICLE FOR EXAMPLES, BUT THESE ARE THE COURSE DEFINITIONS)

• Cause – failure of a device
  • open circuit, short circuit, or change in device behavior
  • for complex devices, could be failure of a particular feature (e.g., caused by “stuck at” fault of microcontroller port pin)
  • list all components that could produce this failure mode
• Mode – related to method of diagnosis
  • observable or measurable behavior of component or sub-circuit resulting from a device failure
  • something you might observe when probing internals of the system with a multi-meter, scope, or logic analyzer
• Effect – external behavior of entire system
  • for thermostat, it either overheats or under-heats the residence
  • for most systems – possibility of fire or damage to other components, external or internal
• Criticality – how serious are the consequences
  • HIGH: involves potential injury, requires rate \( \leq 10^{-9} \)
  • MEDIUM (optional): renders system unrepairable
  • LOW: inconvenience to user, required rate typically \( > 10^{-6} \)
REVISITING THE NEST CASE STUDY

What's Inside
REVISITING THE NEST CASE STUDY

Conceptual Block Diagram
REVISITING THE NEST CASE STUDY

Block Diagram
REVISITING THE NEST CASE STUDY

Basic 4-Wire Circuit Thermostat Circuit

What can go wrong:
1. LCD/backlight fails
   • thermostat continues to function, but nothing is displayed on LCD screen
   • LOW criticality
2. Failure to close control contact
   • no heating/cooling
   • MEDIUM criticality
3. Control contact stuck closed
   • continuous heating or cooling (will not shut off)
   • HIGH criticality (damage to HVAC system and/or personal property, potential health risk)
FMECA ANALYSIS

Identify Potential Failure Modes and Criticality Level
FMECA ANALYSIS

Identify Potential Failure Modes and Criticality Levels
FMECA ANALYSIS

High Voltage Buck Converter

Potential failure modes and effects:
1. PN diode fails open → no power, device inoperative
2. PN diode fails shorted
   - No power, device inoperative
   - AC potentially across capacitors → short circuit/damage
   - HVAC control contact stuck closed → continuous heat/cool
Potential failure modes and effects:
1. Zener diode fails open → (limited effect, may be undetected)
2. Zener diode fails shorted
   - No power, device inoperative
   - HVAC control contact stuck closed
     (circuit draws excessive current) → continuous heat/cool
Potential failure modes and effects:
1. Capacitor fails open → (limited effect, may be undetected)
2. Capacitor fails shorted
   • No power, device inoperative
   • HVAC control contact stuck closed (circuit draws excessive current) → continuous heat/cool
Potential failure modes and effects:

1. Buck regulator fails with $V_{out} = 0$ → thermostat inoperative
2. Buck regulator fails with $V_{out} = V_{in}$
   - Overvoltage to backplate, fry most active components
   - Unpredictable effect on thermostat control contacts
# FMECA Analysis

## High Voltage Buck Converter

<table>
<thead>
<tr>
<th>No.</th>
<th>Failure Mode</th>
<th>Possible Causes</th>
<th>Failure Effects</th>
<th>Detection Method</th>
<th>Criticality</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Vout = 0</td>
<td>open PN diode failed regulator</td>
<td>unable to operate HVAC or charge battery</td>
<td>no current drawn from control contact</td>
<td>MEDIUM</td>
</tr>
<tr>
<td>2</td>
<td>Vout=0</td>
<td>shorted PN diode shorted capacitor shorted zener diode</td>
<td>HVAC stuck on, unable to charge battery</td>
<td>excessive current drawn from control contact</td>
<td>HIGH</td>
</tr>
<tr>
<td>3</td>
<td>Vout &gt; 4.5</td>
<td>failed regulator</td>
<td>Unpredictable effect, potential for component damage</td>
<td>backplate supply voltage &gt; 4.5 V</td>
<td>HIGH</td>
</tr>
</tbody>
</table>
Most electronic thermostats accomplish this function (switching AC signals) using a relay or an (optically isolated) thyristor (triac or SCR) – why is such a complicated circuit used by the Nest Thermostat to perform essentially the same task?

Why is a transformer required?
Why is PWM used?
Why are two MOSFETs required?
Focus on Power MOSFETs

Potential failure modes/effects:
1. Either or both MOSFETs fail open?
   • unable to turn on heating or cooling
   • unpredictable effect if only one MOSFET fails open
2. Either or both MOSFETs fail shorted?
   • heating/cooling stuck on (no way to turn off)
   • unable to harvest energy → battery will discharge
<table>
<thead>
<tr>
<th>No.</th>
<th>Failure Mode</th>
<th>Possible Causes</th>
<th>Failure Effects</th>
<th>Detection Method</th>
<th>Criticality</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>open</td>
<td>open MOSFET gate drive failed off</td>
<td>unable to operate HVAC</td>
<td>open (Hi-Z) control contact</td>
<td>MEDIUM</td>
</tr>
<tr>
<td>2</td>
<td>closed</td>
<td>shorted MOSFET gate drive failed on</td>
<td>HVAC stuck on, unable to charge battery</td>
<td>closed (shorted) control contact</td>
<td>HIGH</td>
</tr>
<tr>
<td>3</td>
<td>partial open</td>
<td>one MOSFET failed open</td>
<td>Unpredictable effect, may not be able to operate HVAC</td>
<td>“half-wave” control contact when “on”</td>
<td>MEDIUM</td>
</tr>
<tr>
<td>4</td>
<td>partial closed</td>
<td>one MOSFET failed closed</td>
<td>Unpredictable effect, HVAC may be stuck on, battery charge current reduced</td>
<td>“half-wave” control contact when “off”</td>
<td>HIGH</td>
</tr>
</tbody>
</table>
If only one of the PN junction diodes (highlighted in red) fails open, possible effects include:

A. nominal effect – may be undetected
B. amount of energy that can be harvested from HVAC control contact is cut in half
C. massive ripple at input to buck converter may result in unpredictable backplate voltage
D. B and C
E. none of the above
If the zener diode (highlighted in yellow) fails open, possible effects include:

A. nominal effect – may be undetected
B. backplate power supply will be 0 V
C. HVAC control contact stuck closed, resulting in continuous heat/cool
D. excessive current drawn from HVAC control contact
E. none of the above
If any of the capacitors (highlighted in blue) fails shorted, possible effects include:

A. nominal effect – may be undetected
B. backplate power supply will be 0 V
C. HVAC control contact stuck closed, resulting in continuous heat/cool
D. B and C
E. none of the above
I can't even begin to say how upset I am to have to title the Nest Learning Thermostat as "The Worst Thermostat EVER." For the "cool" factor and appearance it was in "A" in my book. I installed it in November 2014 and it worked like a charm... for 4 weeks. Then we came home to a house that was 80+ degrees in winter (in Buffalo no less) and found "the base unit was malfunctioning" preventing the nest from shutting off. The "overnight" Fed-Ex replacement arrived in 2 days which meant I had to manually turn on and off the furnace from the circuit breaker. The new nest worked great... for 3 weeks before it did the same thing. Another call to nest with their crazy long wait customer service stated this was a known issue and another unit would be sent... "overnight." Four (4) days later FedEx showed with my third unit in the same number of months and it worked again...well. Yesterday, after only 2 1/2 weeks from install, the Nest again malfunctioned and my phone call to their customer support agent and "senior" agent finally concluded my energy efficient Heil forced air gas furnace was "incompatible" to the nest. What?!?!? I have finally had it and went straight to Home Depot and purchased a Honeywell Smart Thermostat as a replacement. My last Honeywell thermostat lasted over 20 years and I'm just hopeful this one will last longer than the Nest's.
• Failure Mode, Effects, and Criticality Analysis (FMECA)

- **Failure Modes:** Divide your schematic into functional blocks (e.g., power circuits, sensor blocks, microcontroller block) – include this illustration as Appendix A. Break the schematic into small enough blocks so that details are readable. Determine all possible failure conditions of each functional block. Indicate the components that could possibly be responsible for such a failure (e.g., a shorted bypass capacitor might cause a voltage drop, but cannot cause a voltage increase).

- **Effects:** For each failure mode above, determine the possible effects, if any, on any major components in other parts of the design (e.g., damage the microcontroller or fry a resistor) as well as effects on the overall operation of the project (e.g., audio volume increases to maximum). For some failure modes, it is acceptable to declare the effects unpredictable. “Method of detection” of a particular failure mode should be observable from the operation of the device, unless there is particular circuitry intended to detect such a failure.

- **Criticality:** Begin by defining at least two criticality levels for types of failures in the output of your design. Define an acceptable failure rate $\lambda$ for each level of failure. These are up to you and somewhat arbitrary, but keep in mind $\lambda < 10^{-9}$ is standard for any failure that could potentially injure the user. Failures not affecting user safety do not usually require $\lambda < 10^{-9}$.

- **FEMCA Worksheet:** Include your completed FEMCA Worksheet as Appendix B. In the body of the report, explain your choice of criticality levels and any assumptions that affected your analysis of several failure modes. Assumptions affecting just individual failure modes can be included in the comments in the table.
SOFTWARE RELIABILITY

Revisiting How Nest Learns

Senses and learns from you.

The Nest Thermostat integrates information from its sensors and the outside weather.

**Activity sensors**
Nest’s activity sensors have a 150° wide-angle view. That range enables Nest to activate Auto-Away in 90% of homes.

**Humidity sensor**
Nest shows you indoor humidity and can manage your whole-home humidifier or dehumidifier.

**Temperature sensors**
Three temperature sensors track your home’s temperature and how quickly it changes.

**Weather aware**
Nest uses its Wi-Fi connection to keep an eye on current weather conditions and forecasts so it can understand how the outside temperature affects your energy use.
**SOFTWARE RELIABILITY**

**Discussion**

- Potential non-determinism associated with multithreaded software
  - Large set of input variables (sensors) and states
  - Effect of sensor malfunction on learning ability and impact on program behavior
    - Potential to learn “bad habits”?  
    - Ability to recognize and “clear” incorrectly learned behavior?
  - Standard testing may not reveal latent software bugs

---

**The Problem of Non-Determinism**

Multithreaded software is non-deterministic. Some executions may exhibit a bug, e.g., a deadlock, while others may not. Standard testing may therefore not reveal the bug.

**The Solution of Runtime Analysis**

Runtime analysis examines a single execution trace for the “footprints” of bugs, e.g., cycles in a lock graph. A bug usually leaves prints in most execution traces, even if the executions do not exhibit the bug.

**Our Improved Runtime Analysis Algorithm**

Standard runtime analysis of deadlocks yields false positives. New algorithm reduces number of false positives by using labeled lock graphs.

---

**Case Study Results**

- **K9 rover**: Found one unexpected deadlock, confirmed one data race, and found all seeded deadlocks and data races.
- **DS1 Attitude Control System**: Found two unexpected data races, and all seeded data races.
FAILURE REPORTS

Customer Complaints Documenting That Software Failures Can and Do Occur

• “The NEST product was an interesting and fun gadget for a year and a half ... until control of it was taken away by someone during one of the coldest days of the year. As the house got colder and colder I worked through the NEST website looking for tech support to no avail. Finally Googling "NEST help" got me a contact number. During three hours of troubleshooting I found out that this thermostat was part of an energy savings program. NEST thought the thermostat was controlled by my local utility. I contacted my local utility and they had no idea what I was talking about. I then went back to NEST and they still had no idea who was controlling the thermostat or how low the "Controller" whoever that was would let the temp fall. I worked with them a little longer in an attempt to opt out of this energy saving program and after three hours I told them thank you very much, but your time is up. I then replaced this thermostat with a conventional programmable thermostat. The NEST product is not ready for prime time.”

• WOWWW The coldest day of the year, this is the second time NEST shut down heating system and said it wanted us to call nest service to come fix heating system. I had to reconnect old thermostat which corrected the issue. what a scam ;;;; im wondering who had control of my house ???
SOFTWARE RELIABILITY

Watchdog Timer

• Role of watchdog timer is to reset processor if “strobe timeout” occurs
• **Problem**: watchdogs integral to microcontroller are no more reliable than microcontroller itself
• External watchdogs “better”, but have to make sure that it is prevented from being strobed in the event of failures/bugs
• **Possible solution**: make watchdog respond to a “key” (that would be difficult for failed software/bug to generate)
THE REST OF THE STORY...

- Designing a functional product represents about 30% of the design effort
- Making sure a product always fails in a safe, predictable manner takes the remaining 70%
- Law of diminishing returns: exercise good judgment in adding safety features
- Keep in balance: safety features and possibility of “nuisance alarms” (failures resulting from added complexity)
- Utilize built-in self-test (BIST)

FIGURE 1. Autonomous BIST
MAINTAINABILITY

- Reliability predication indicates how many problems per day will need to be serviced after, say, 10,000 units have been shipped
- Keep customers happy with quick repair turn-around time (TAT)
- Repair will most likely be by replacement (“line replaceable units” – LRU)
- Maintainability analysis generates data showing the time needed to identify the faulty LRU, the time to replace it, and the time to re-test the system
- Mean-time-to-repair (MTTR)
STANDARDS AND COMPLIANCE

Example Category Relevant to ECE 477 Projects


Hazard Based Safety Engineering

Energy sources: electrical, thermal, kinetic, and radiated

To prevent pain or injury, either the energy source can be designed to levels incapable of causing pain or injury, or safeguards such as insulation can be designed into the product to prevent energy transfer to the body part.
CLICKER QUIZ

Question 8

Find the number of (obvious) errors in the power supply schematic shown:

A. 0
B. 1
C. 2
D. 3
E. > 3

Source: Circuit Cellar April 2016 Electrical Engineering Challenge Circuit.