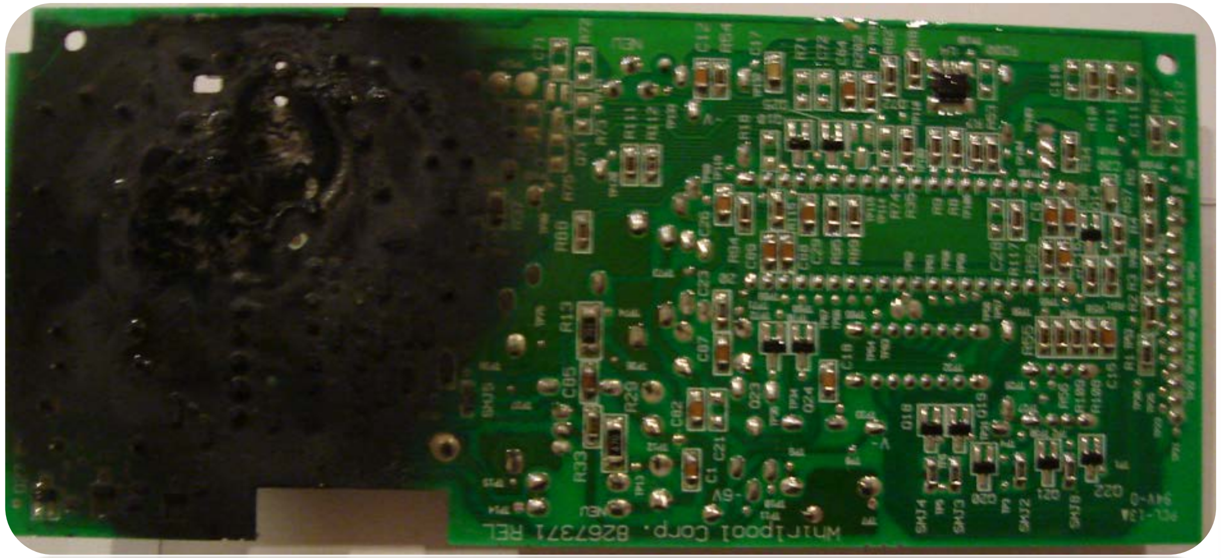
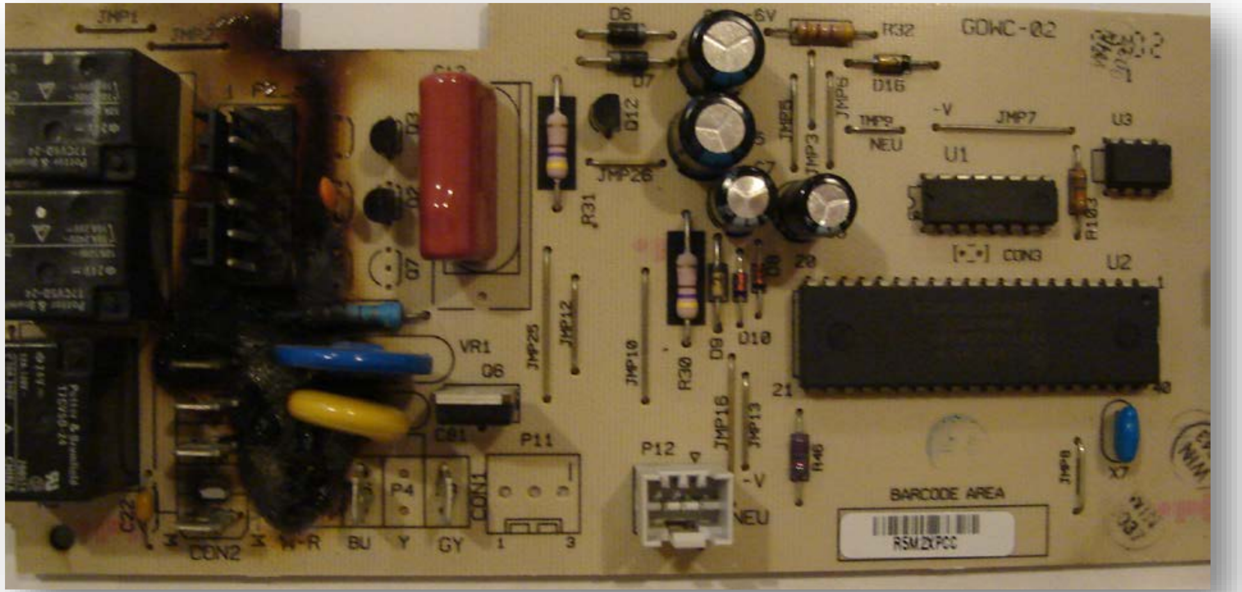
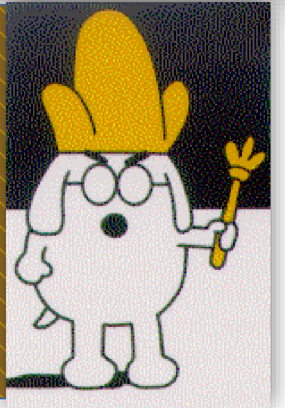




Professional Considerations in Digital System Design

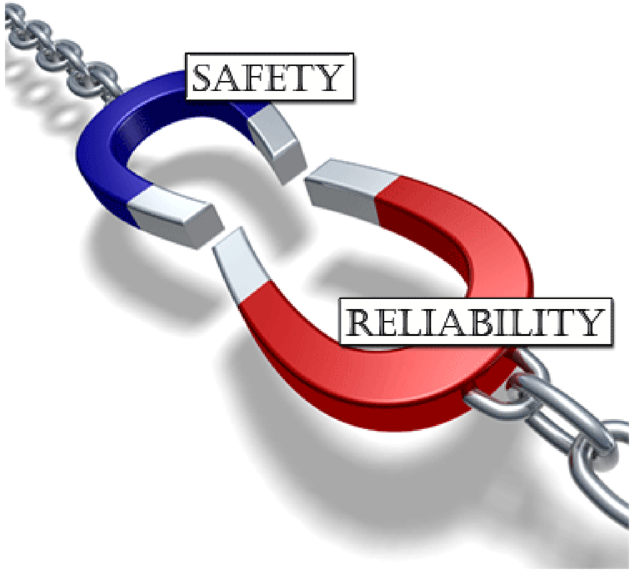
RELIABILITY AND SAFETY ANALYSIS



PURDUE
UNIVERSITY

OUTLINE

- Introduction
- Component Failures and Wear
- Definition of Failure Rate
- Critical Role of Bypass Capacitors
- Reliability Models for Components
- Mean Time To/Before Failure (MTTF/MTBF)
- Failure Mode & Effects Analysis (FMEA)
- Criticality Analysis (FMECA)
- Electromechanical Failures
- Revisiting the Nest Case Study
- Software Reliability
- Maintainability
- Standards and Compliance

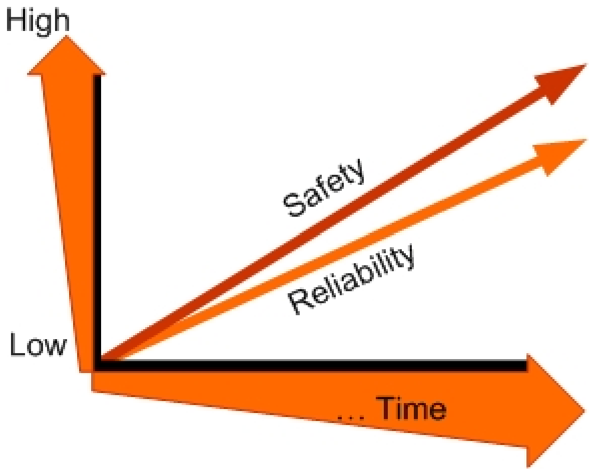


Reference: "Designing for Reliability, Maintainability, and Safety – Parts 1, 2, and 3", Circuit Cellar, December 2000, January 2001, April 2001.

PURDUE UNIVERSITY

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

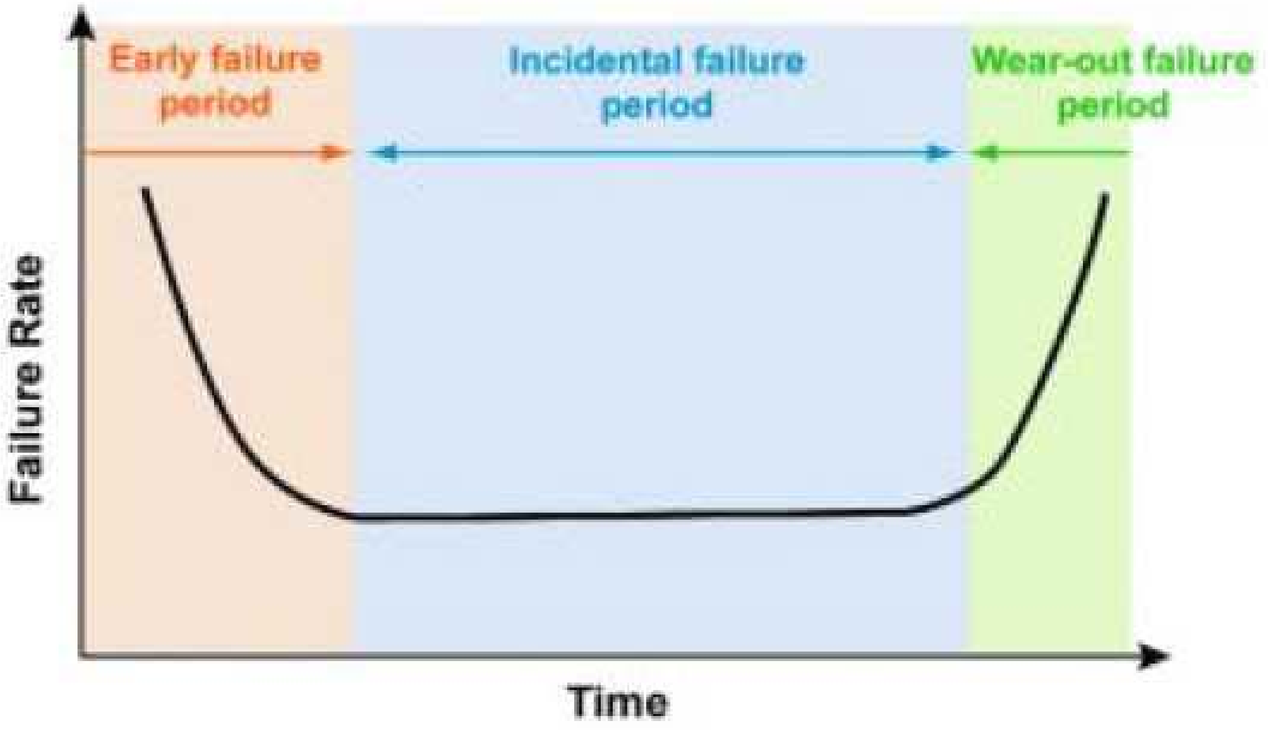


PURDUE
UNIVERSITY

COMPONENT FAILURES AND WEAR

- Electronic components can most often be modeled by constant failure rate (λ)*
- 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"

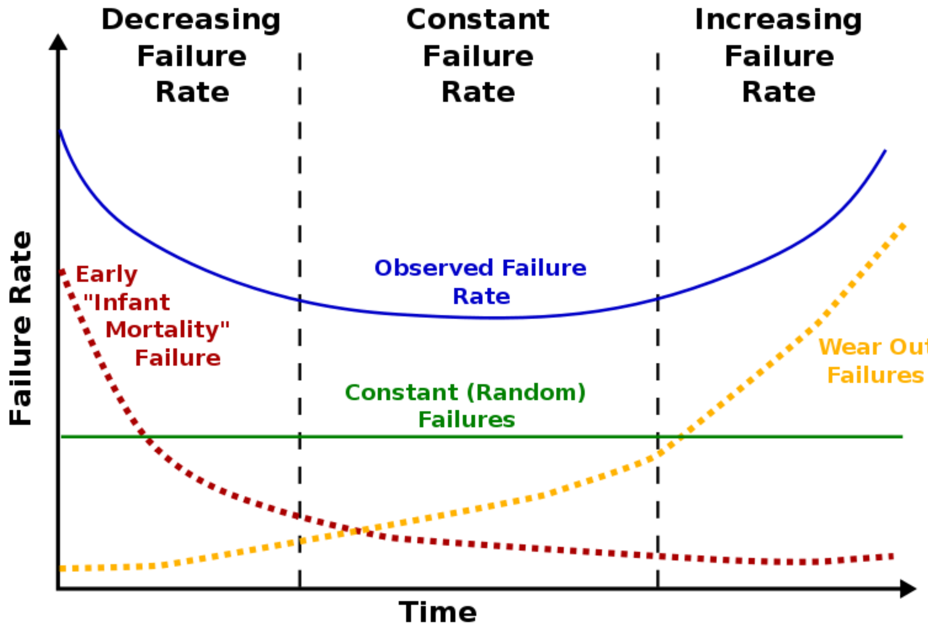
***but…see also May 2011 *IEEE Spectrum* feature article on "Transistor Aging"**



PURDUE UNIVERSITY

COMPONENT FAILURES AND WEAR

- 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"



PURDUE UNIVERSITY

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. [fails/(10^6 hour $\times$ unit)]
- 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)

PURDUE UNIVERSITY

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)
  - 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 = 2×10^{-6} fails/(hr $\times$ unit) $\times$ 1000 units $\times$ (365 $\times$ 24) hours = 17.52

PURDUE UNIVERSITY

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$) =$ 0.595×10^{-6} failures per unit per hour

PURDUE UNIVERSITY

PERSPECTIVE

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

PURDUE UNIVERSITY

PERSPECTIVE

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 1×10^{-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)

PERSPECTIVE

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

PERSPECTIVE

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

* If rate is <u>not</u> acceptable, what would be an appropriate "high criticality" failure rate, i.e., what would be your definition of "never"?

10^{-9}

PURDUE UNIVERSITY

COMPONENT WEAR

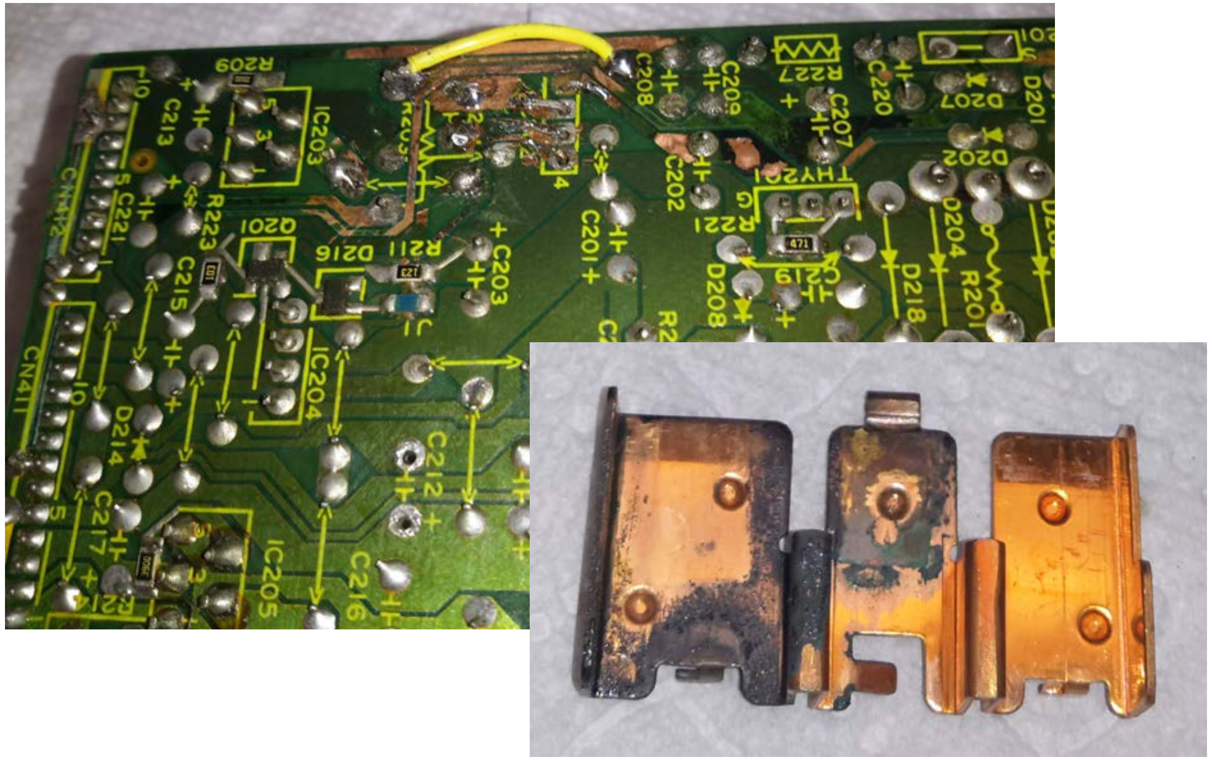
- If, based on observation, failure rate does depend on time used, it may be due to wear caused by *improper derating*
- See also "An Odometer for CPUs," *IEEE Spectrum*, May 2011
- Well-derated electronic systems seldom reach the point of wear-out failure (more discussion of electro-mechanical failures later, though)
- 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

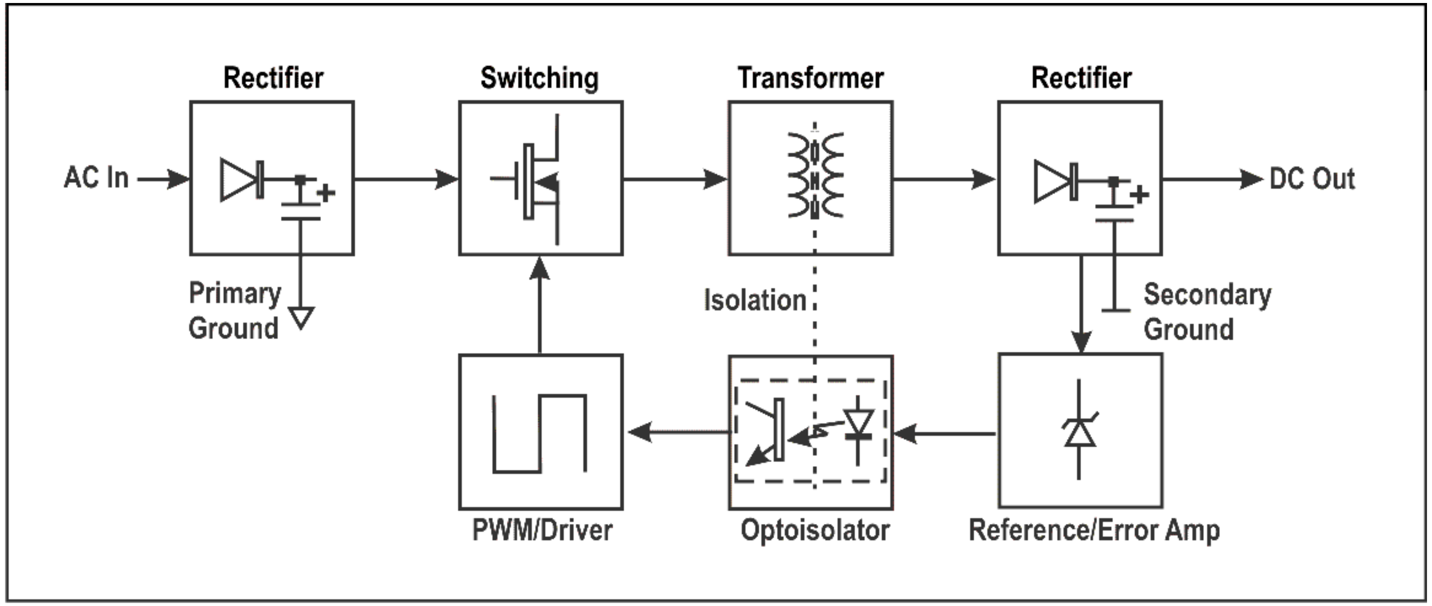
- Heat is the main reliability killer – even a small reduction will have a significant effect
- Components like electrolytic capacitors can “dry out” and deteriorate over time (and/or become “leaky”)

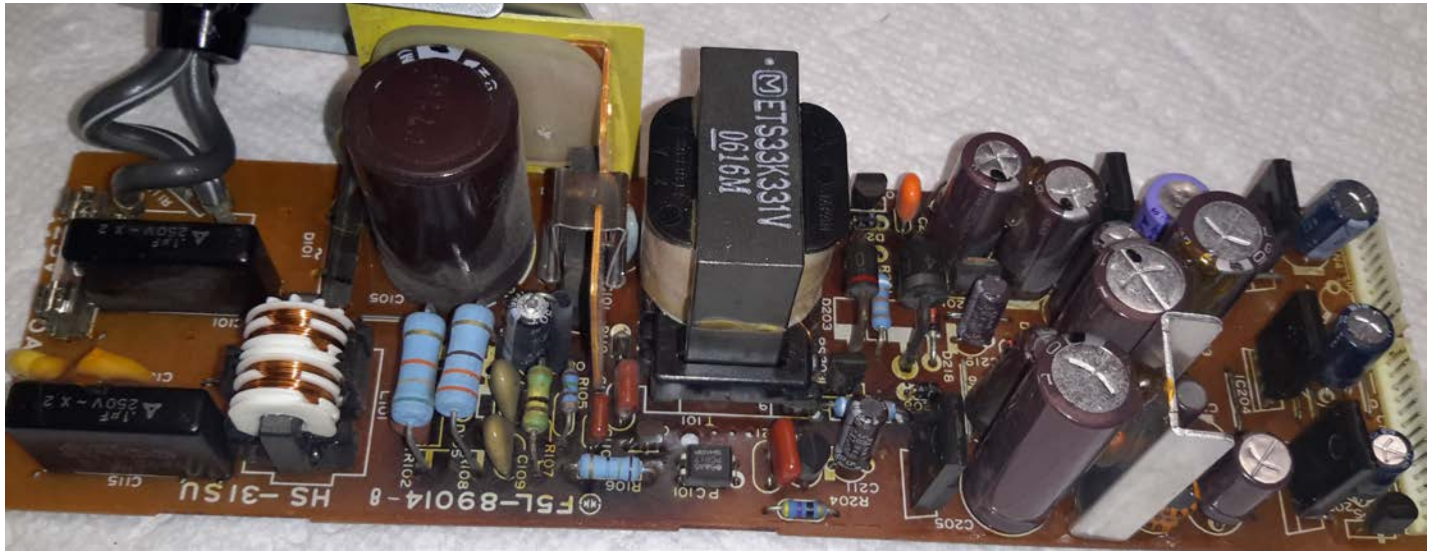
Leaked electrolyte is highly corrosive!



PURDUE
UNIVERSITY

COMPONENT WEAR

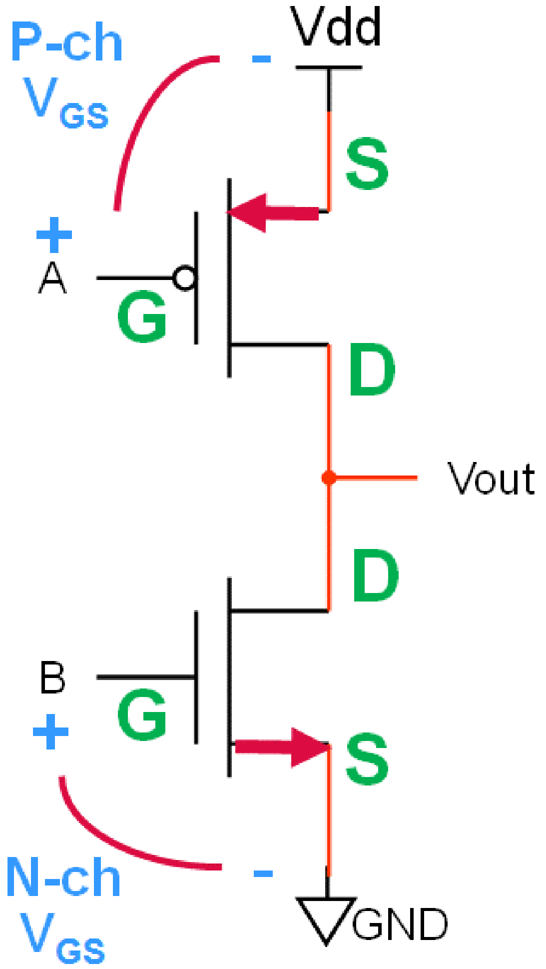


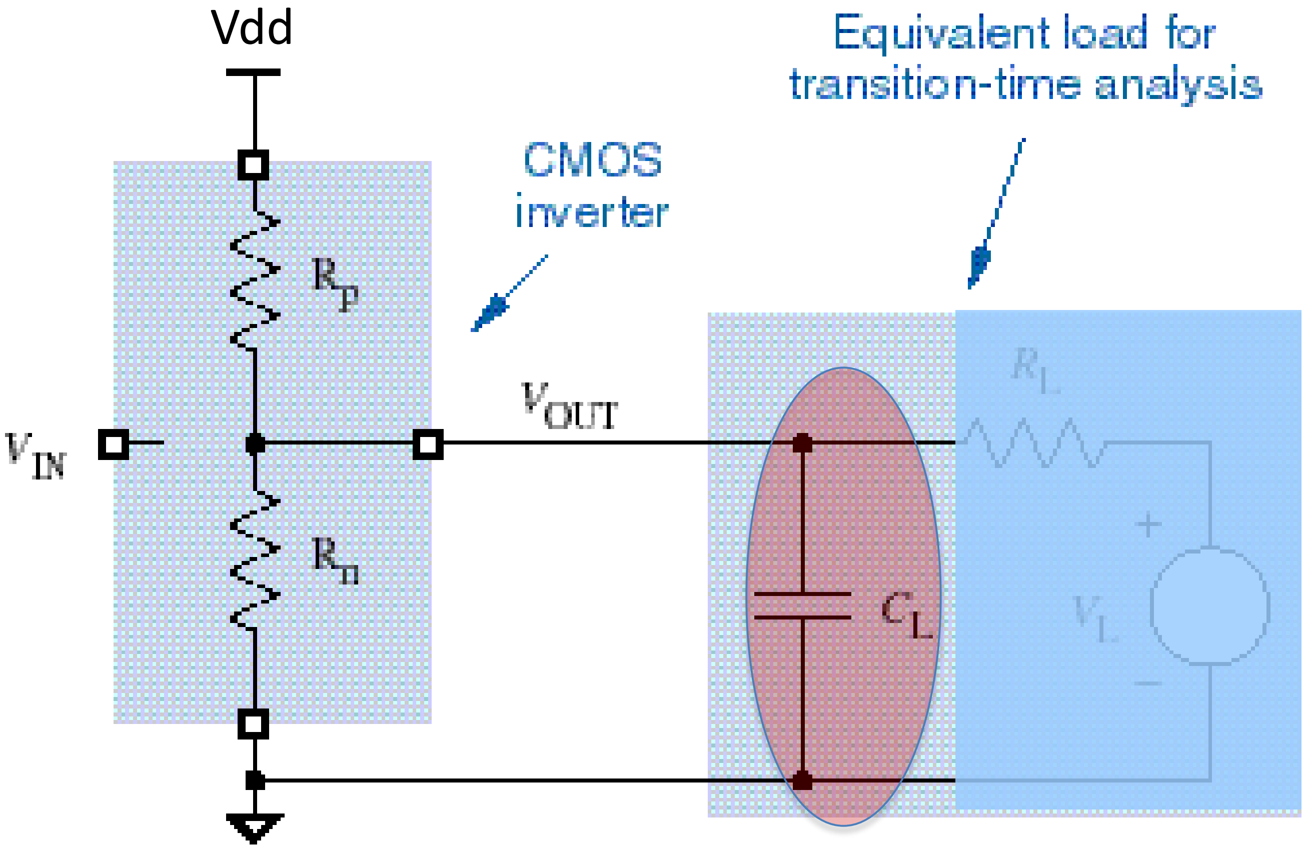


*Electrolytic capacitors used in switch-mode power supplies of this type must be "**high temperature**"* (105° C) *class*

PURDUE
UNIVERSITY

CRITICAL ROLE OF DECOUPLING CAPACITORS





AC component of load

DC component of load

PURDUE UNIVERSITY

CRITICAL ROLE OF DECOUPLING CAPACITORS

- When a CMOS gate output changes state, the P- and N-channel transistors are both partially on simultaneously, causing a *current spike* which shows up as noise on the power and ground traces
- *Decoupling capacitors* must be distributed throughout a PCB to serve as a source of instantaneous current during output transitions – *this helps mitigate noise and improve signal quality*
- All decoupling capacitors should be located as *physically close* as possible to each IC, between each pair of power and ground pins
- Use 0.1 μF decoupling capacitors for system frequencies up to 15 MHz, and 0.01 μF for frequencies greater than 15 MHz

PURDUE
UNIVERSITY

Also include a "bulk" capacitor (10 μF) to provide a local source of current for recharging the decoupling capacitors

RELIABILITY MODELS FOR COMPONENTS

- Calculated value is λ_p, the predicted number of failures per 10^6 hours of operation
- Examples (MIL-HDBK-217F):

Somewhat dated, but publically available

Diodes

$$\lambda_P = \lambda_b \times \pi_T \times \pi_T \times \pi_S \times \pi_C \times \pi_Q \times \pi_E$$

where:

λ_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.

π_T = temperature coefficient; 3.9 for junction temperature T_j < 70°C.

π_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.

π_C = contact construction factor; 1.

π_Q = 8.0 for plastic encapsulated devices.

π_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

(based on # of gates or transistors or on "size" of micro, e.g. 8-bit, 16-bit, etc.)

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

where:

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

π_T = temperature coefficient. Assuming the junction temperature T_j < 100°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.

π_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.

π_L = learning factor; 1 for ICs more than two years in production.

π_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.

PURDUE UNIVERSITY

RELIABILITY MODELS FOR COMPONENTS

PN Junction Diode (Power Rectifier Application)

Parameter	Description	Value	Comments
λ_D	Diode type/application	0.0030	Power rectifier
π_T	Temperature factor	1.0	$T_J = 25° C$
π_S	Electrical stress factor	0.29	$0.4 < V_S \leq 0.5$
π_C	Contact construction	1.0	Metallurgically bonded
π_Q	Quality factor	8.0	Plastic case
π_E	Environmental factor	1.0	G_B

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

PURDUE UNIVERSITY

Reference: MIL-HDBK-217F, pp. 6-2 – 6-3.

RELIABILITY MODELS FOR COMPONENTS

Silicon MOSFET (Power Switching Application)

Parameter	Description	Value	Comments
λ_b	Base failure rate	0.012	MOSFET
π_T	Temperature factor	1.0	T_J = 25° C
π_A	Application factor	2.0	Power FET
π_Q	Quality factor	8.0	Plastic case
π_E	Environmental factor	1.0	G_B

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

PURDUE UNIVERSITY

Reference: MIL-HDBK-217F, p. 6-8.

RELIABILITY MODELS FOR COMPONENTS

CMOS Switch-Mode Regulator IC (8 pin)

Parameter	Description	Value	Comments
C_1	Number of transistors	0.040	300 < x < 1000
π_T	Temperature factor	0.1	CMOS, T_J = 25° C
C_2	Package failure rate	.0013	8-pin flatpack
π_E	Environmental factor	0.5	G_B
π_Q	Quality factor	2.0	Class B-1
π_L	Learning factor	1.0	≥ 2 years

$$\lambda_P = (C_1 \times \pi_T + C_2 \times \pi_E) \times \pi_Q \times \pi_L = 9.3 \times 10^{-8}$$

PURDUE UNIVERSITY

Reference: MIL-HDBK-217F, p. 5-1.

RELIABILITY MODELS FOR COMPONENTS

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

Parameter	Description	Value	Comments
C_1	Die complexity	0.28	16-bit CMOS
π_T	Temperature factor	0.1	CMOS, $T_J = 25°$ C
C_2	Package failure rate	.08724*	80-pin flatpack
π_E	Environmental factor	0.5	G_B
π_Q	Quality factor	2.0	Class B-1
π_L	Learning factor	1.0	≥ 2 years

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

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

PURDUE UNIVERSITY

Reference: MIL-HDBK-217F, p. 5-1.

CLICKER QUIZ

Question 1

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

CLICKER QUIZ

Question 2

The failure rate λp 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

CLICKER QUIZ

Question 3

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

PURDUE UNIVERSITY

CLICKER QUIZ

Question 4

Assuming your design goal is no more than *one unit failure per week* with 10,000 units in the field, an acceptable failure rate (λp) would be approximately:

A. 1×10^{-4}
B. 1×10^{-6}
C. 6×10^{-7}
D. 6×10^{-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)

RELIABILITY & SAFETY ANALYSIS REPORT

- 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. <u>State the model used and any assumptions you had to make</u>. For each component you analyzed, present the parameters you used and the results obtained in a tabular format like the following:*

Parameter	Description	Value	Comments
C_1	Die complexity	0.28	16-bit CMOS
π_T	Temperature factor	0.1	CMOS, T_J = 25° C
C_2	Package failure rate	.08724*	80-pin flatpack
π_E	Environmental factor	0.5	G_B
π_Q	Quality factor	2.0	Class B-1
π_L	Learning factor	1.0	≥ 2 years

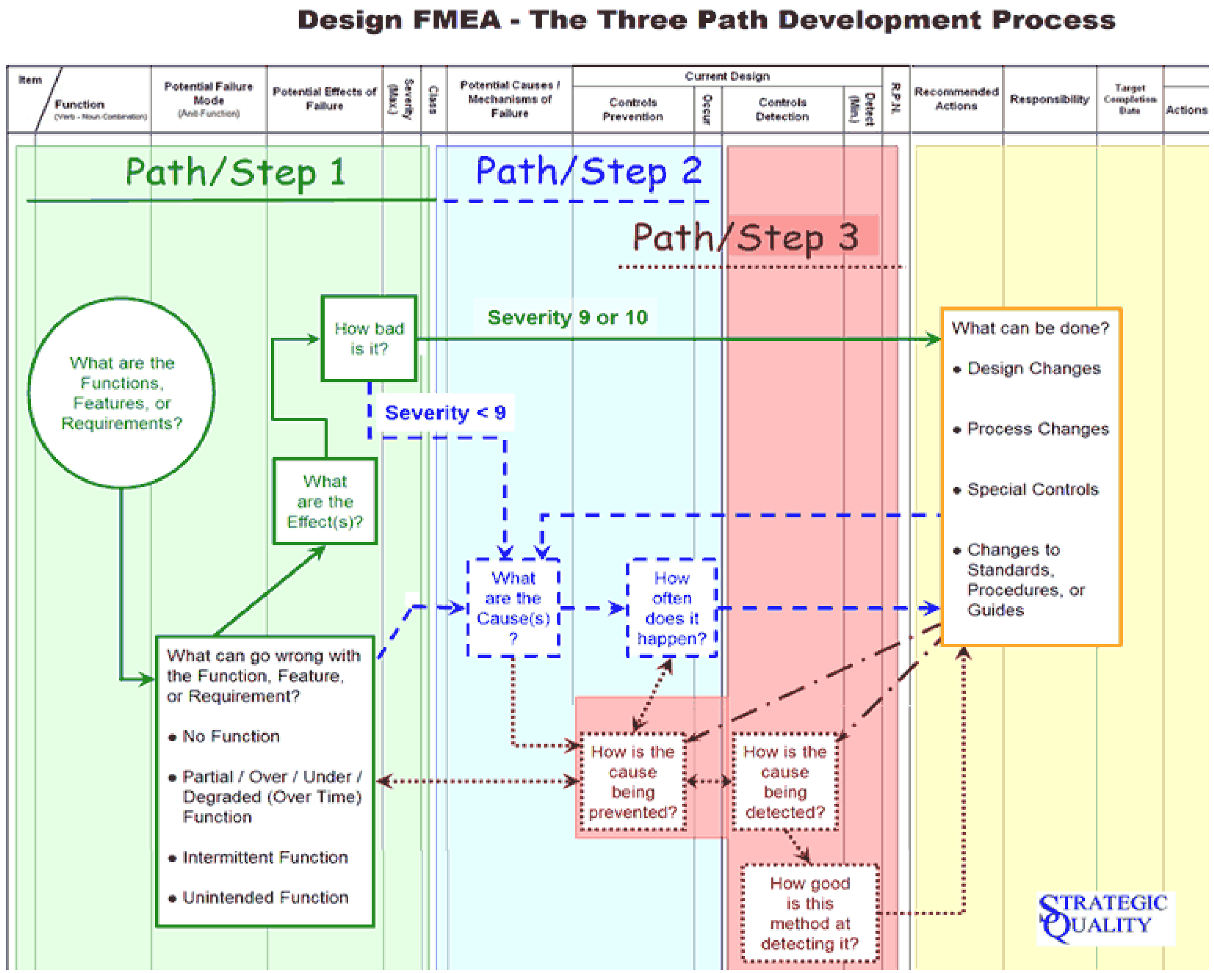
Comments regarding choice of parameter value, especially if you had to make assumptions

  - *Summarize conclusions about the reliability of these components and/or the circuit in general. <u>Suggest design or analysis refinements that would realistically improve the reliability of the design.</u>*

PURDUE UNIVERSITY

FMEA

- <u>F</u>ailure <u>M</u>ode <u>E</u>ffects <u>A</u>nalysis
- 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



FMECA

- 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*

PURDUE UNIVERSITY

* probability calculation not required for homework

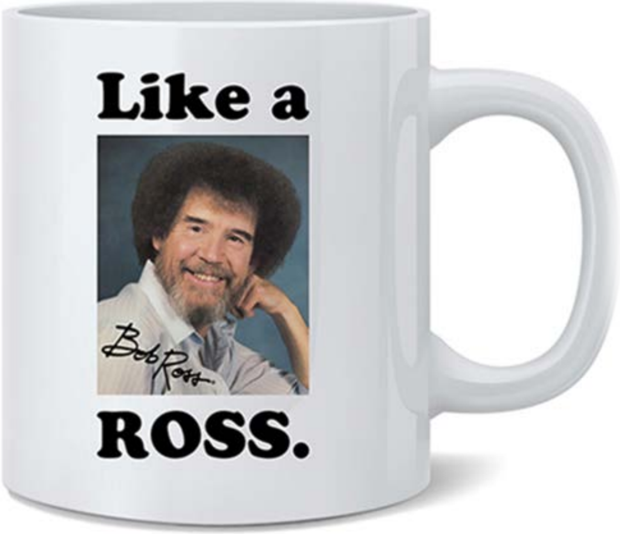
FAILURE CAUSE/MODE/EFFECT/CRITICALITY

(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 $> 10^{-6}$

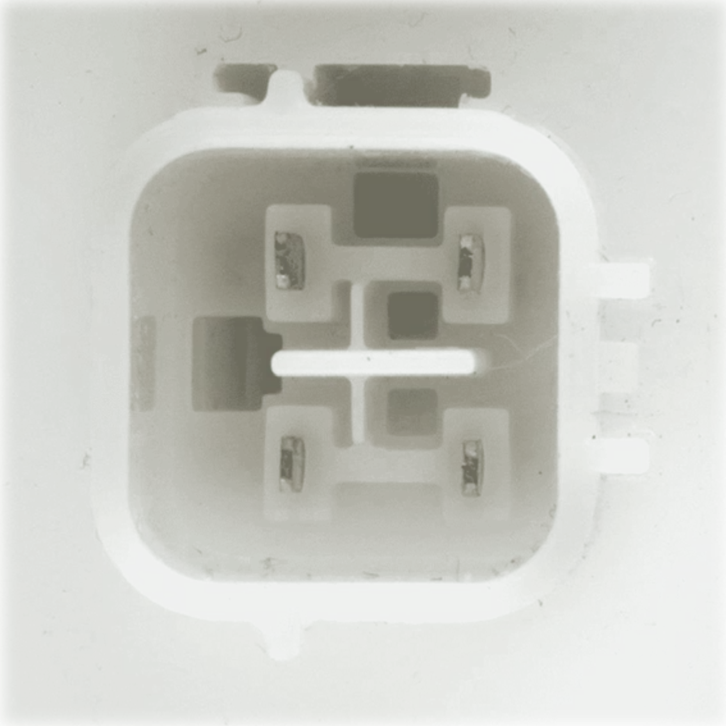
PURDUE UNIVERSITY

Break Time!



ELECTROMECHANICAL FAILURES

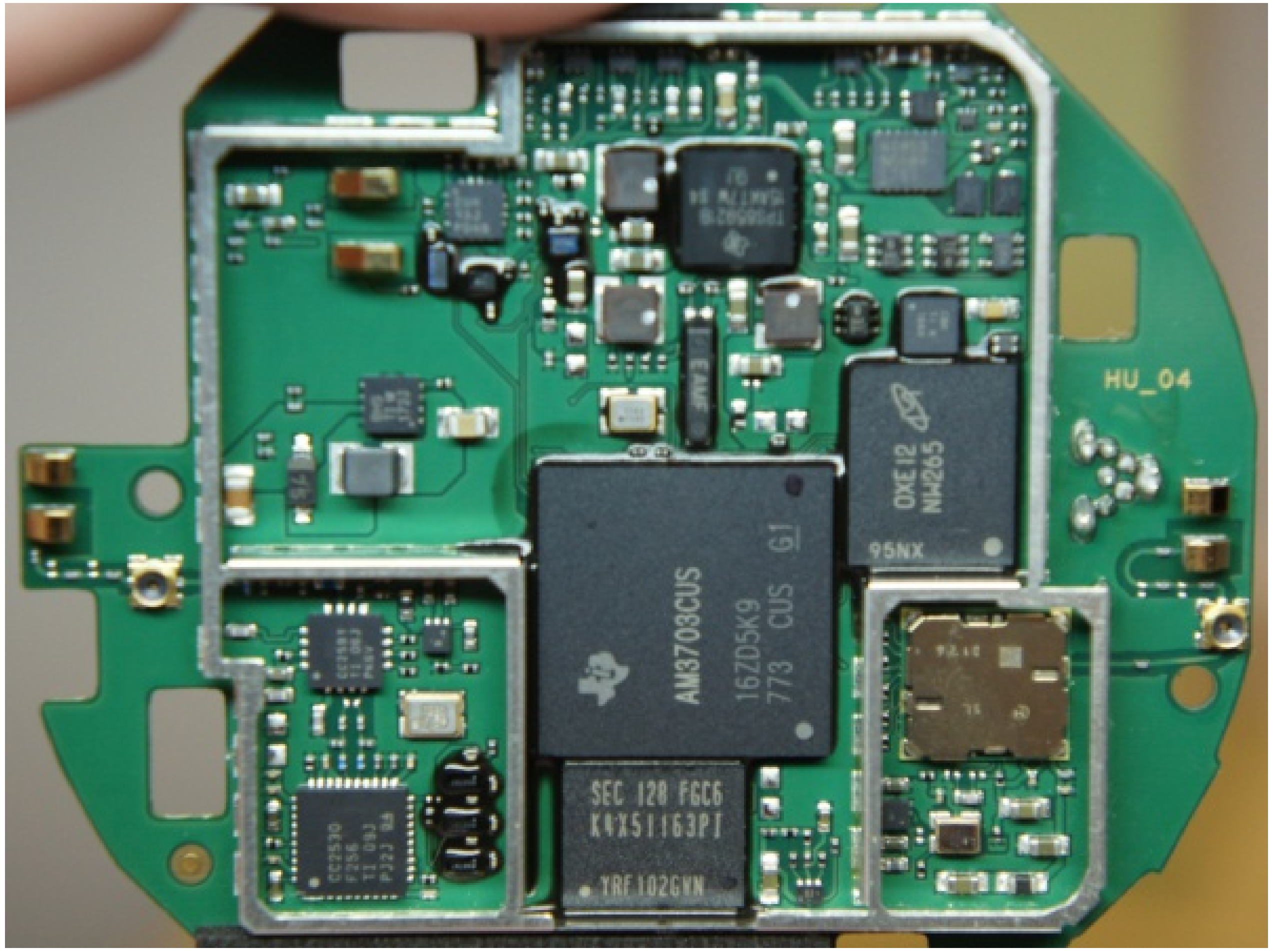
What is it, how did it fail, and what were the potential consequences?

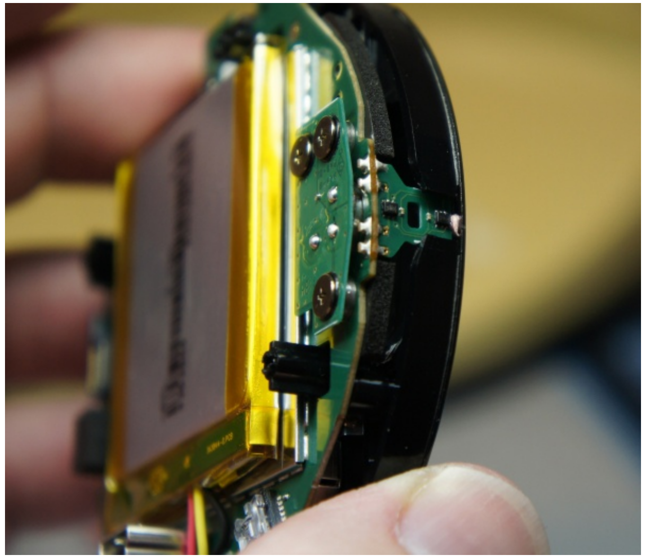


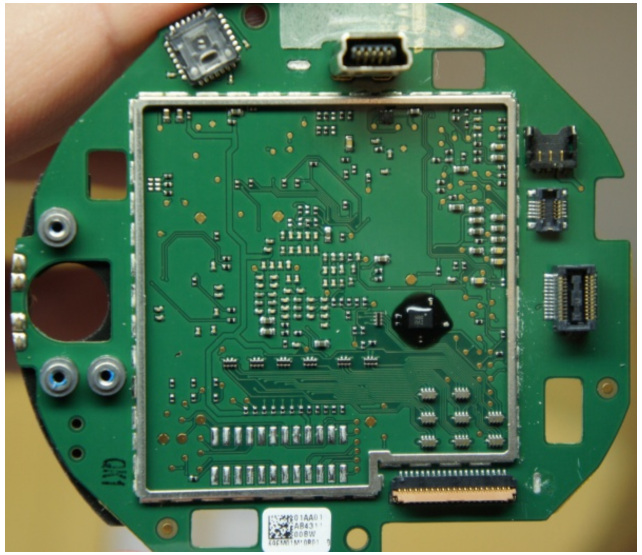
PURDUE
UNIVERSITY

REVISITING THE NEST CASE STUDY

What's Inside



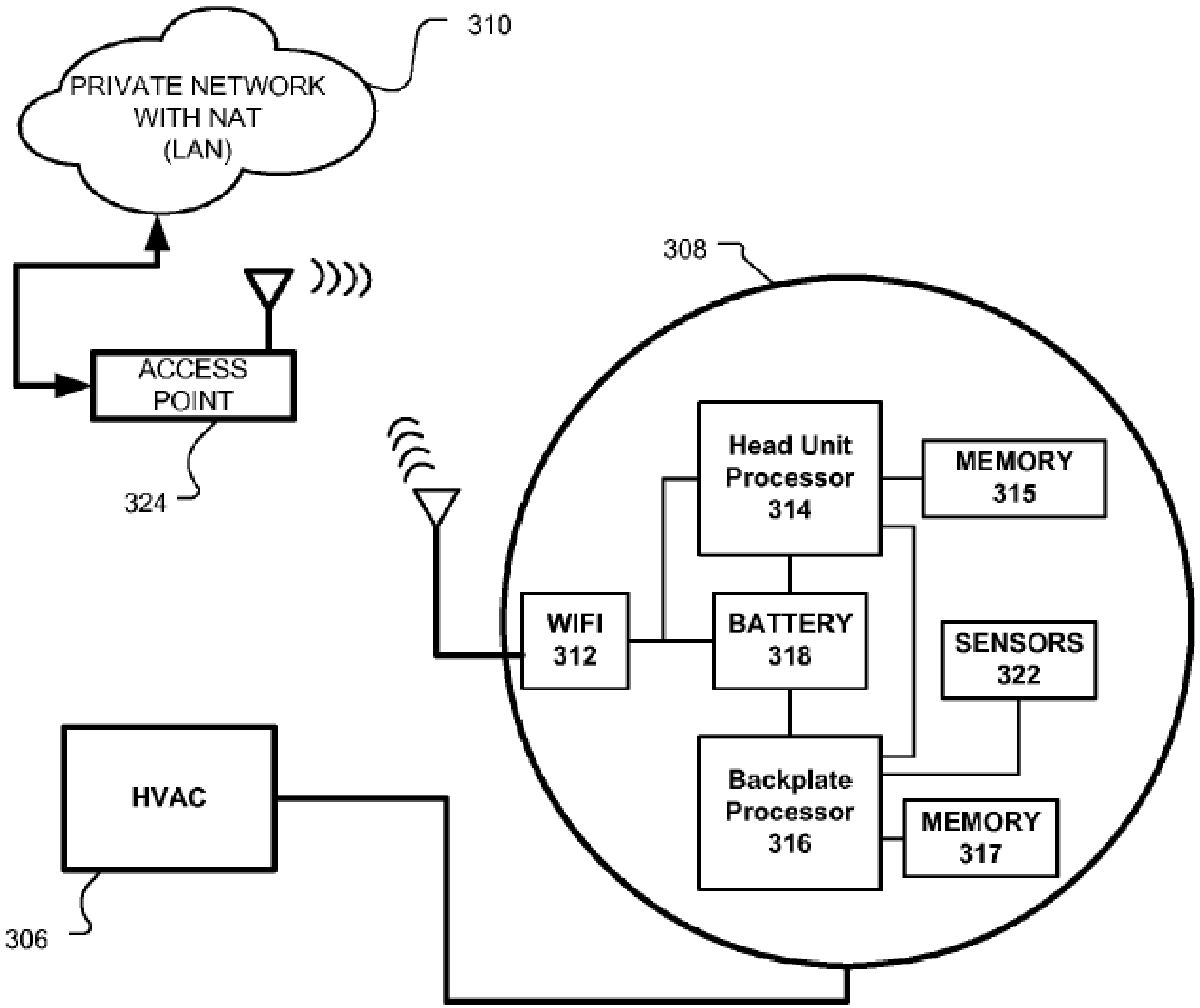




PURDUE
UNIVERSITY

REVISITING THE NEST CASE STUDY

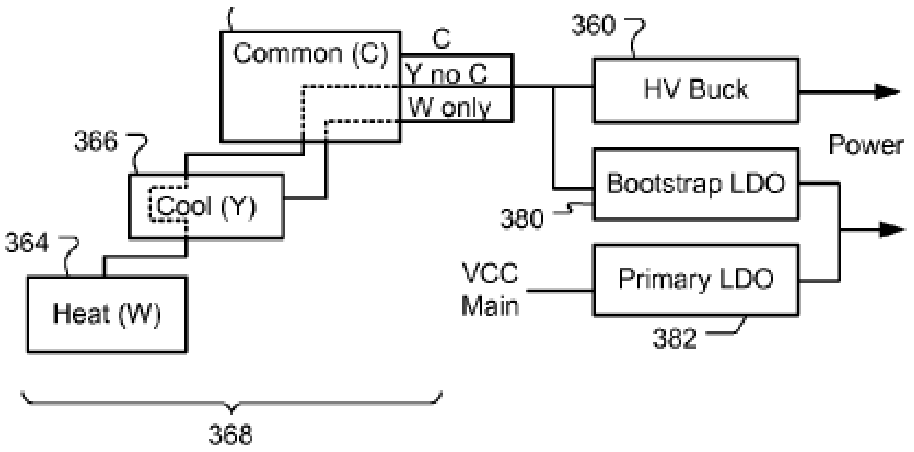
Conceptual Block Diagram

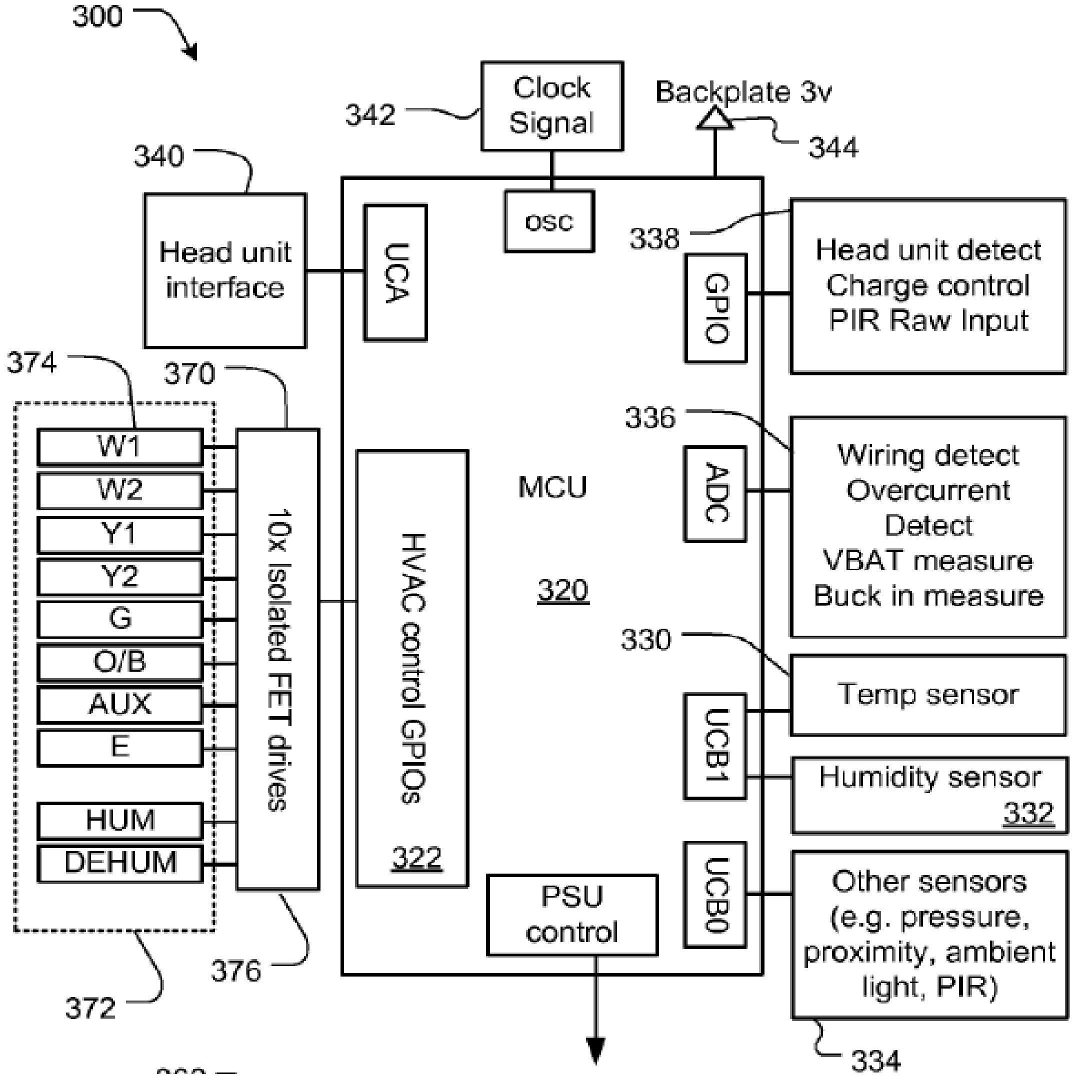


PURDUE UNIVERSITY

REVISITING THE NEST CASE STUDY

Block Diagram

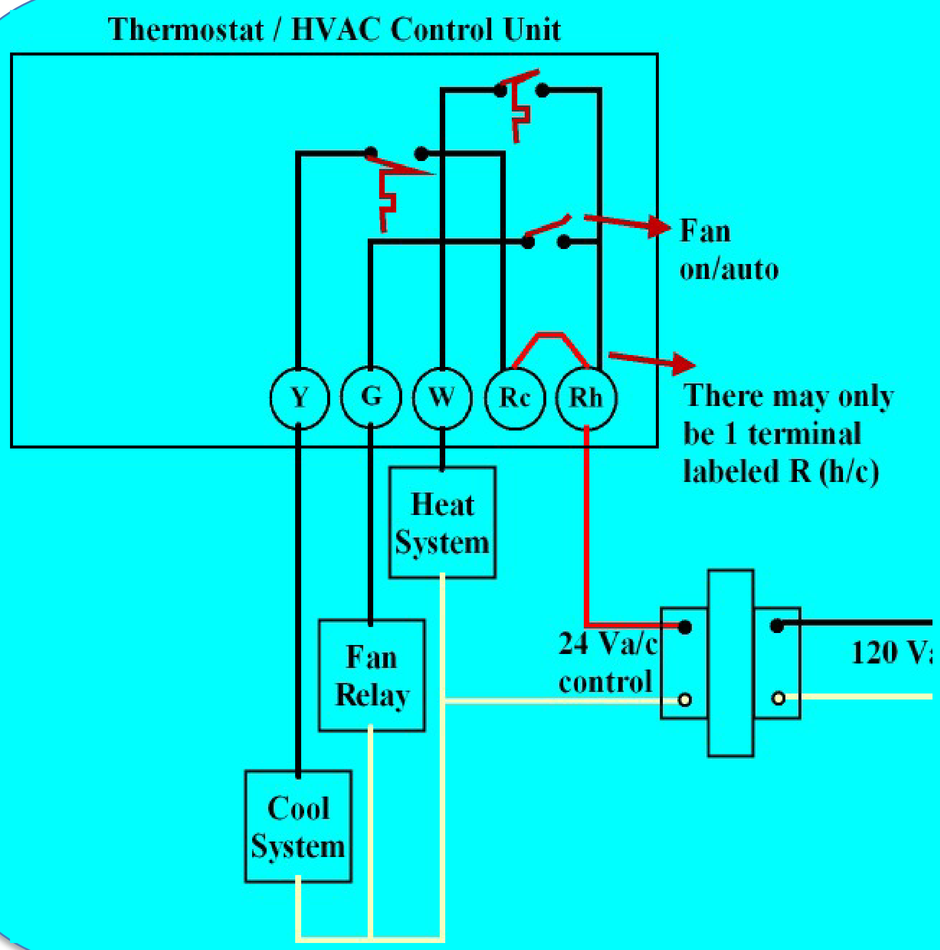




PURDUE
UNIVERSITY

REVISITING THE NEST CASE STUDY

Basic 4-Wire Circuit Thermostat Circuit



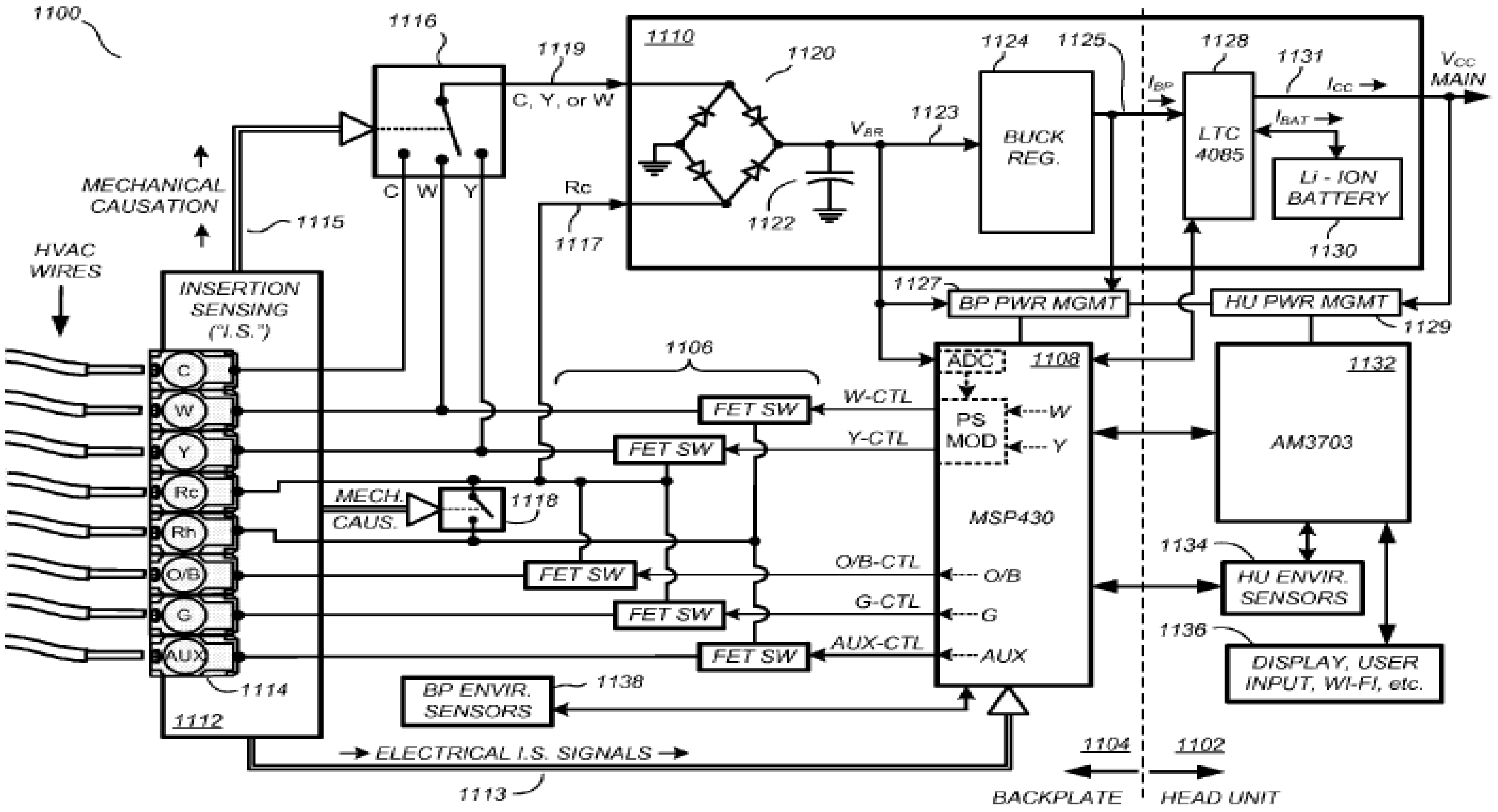
What can go wrong:

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)

PURDUE UNIVERSITY

FMECA ANALYSIS

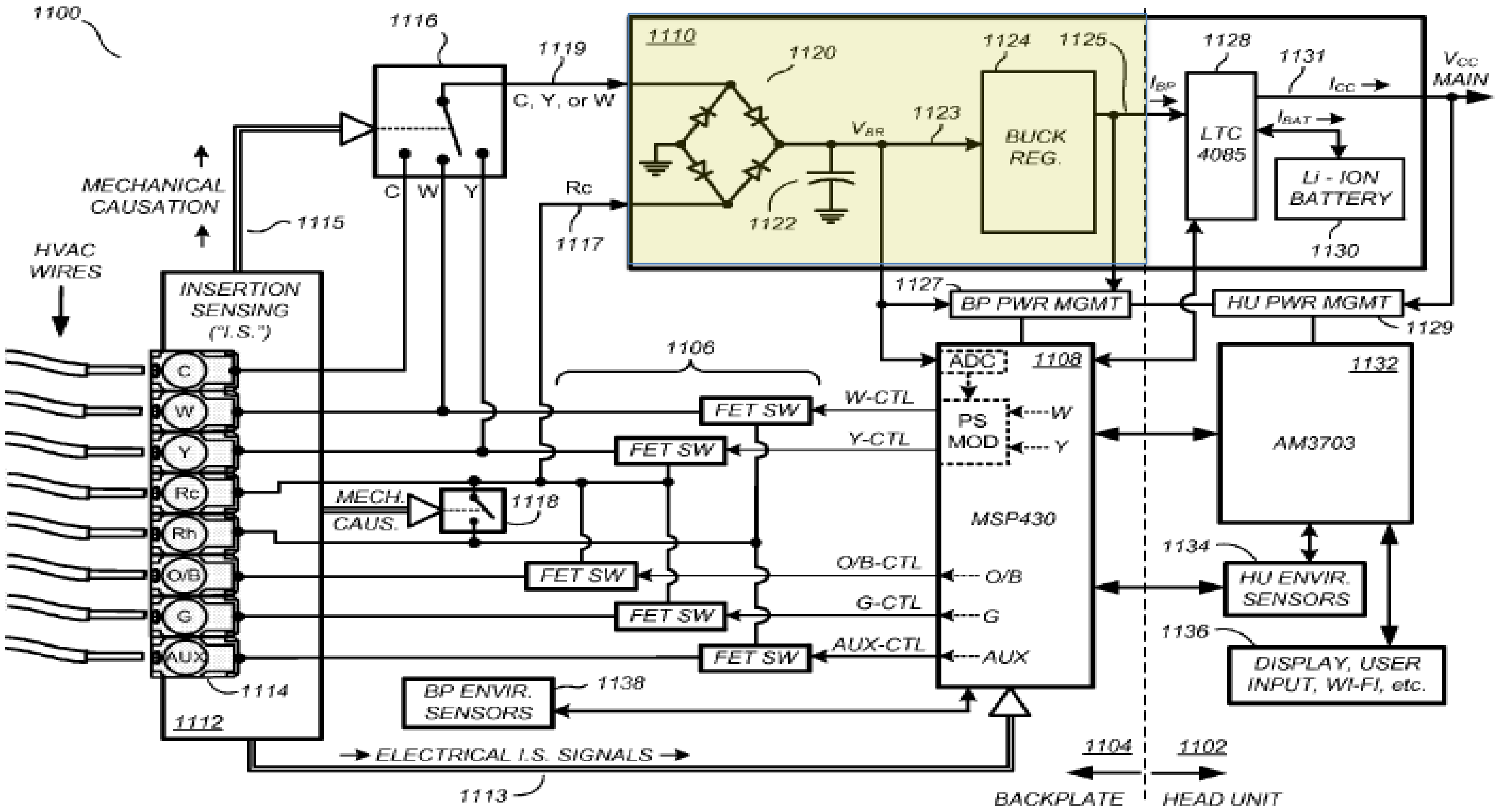
Identify Potential Failure Modes and Criticality Level



PURDUE UNIVERSITY

FMECA ANALYSIS

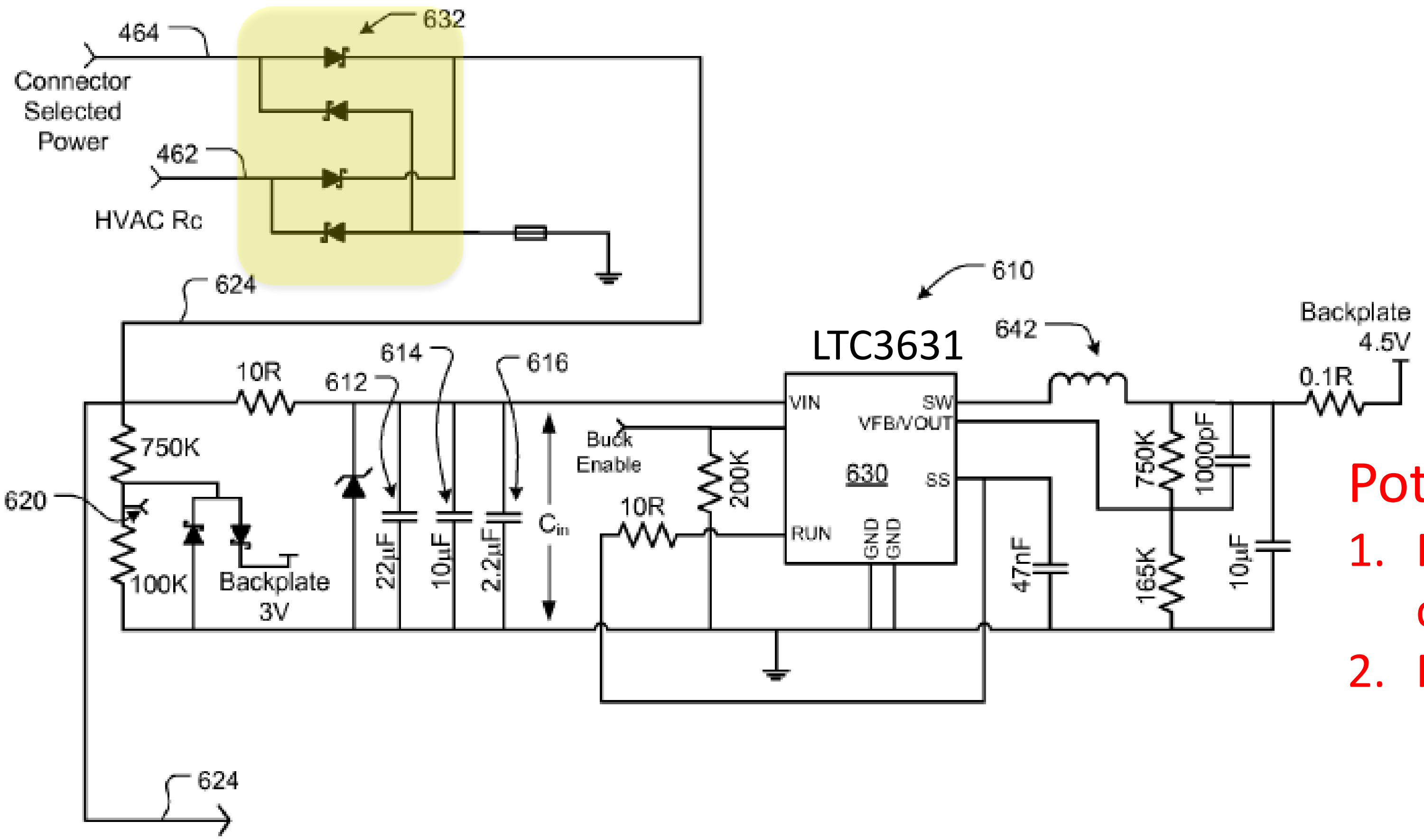
Identify Potential Failure Modes and Criticality Levels



PURDUE UNIVERSITY

FMECA ANALYSIS

High Voltage Buck Converter



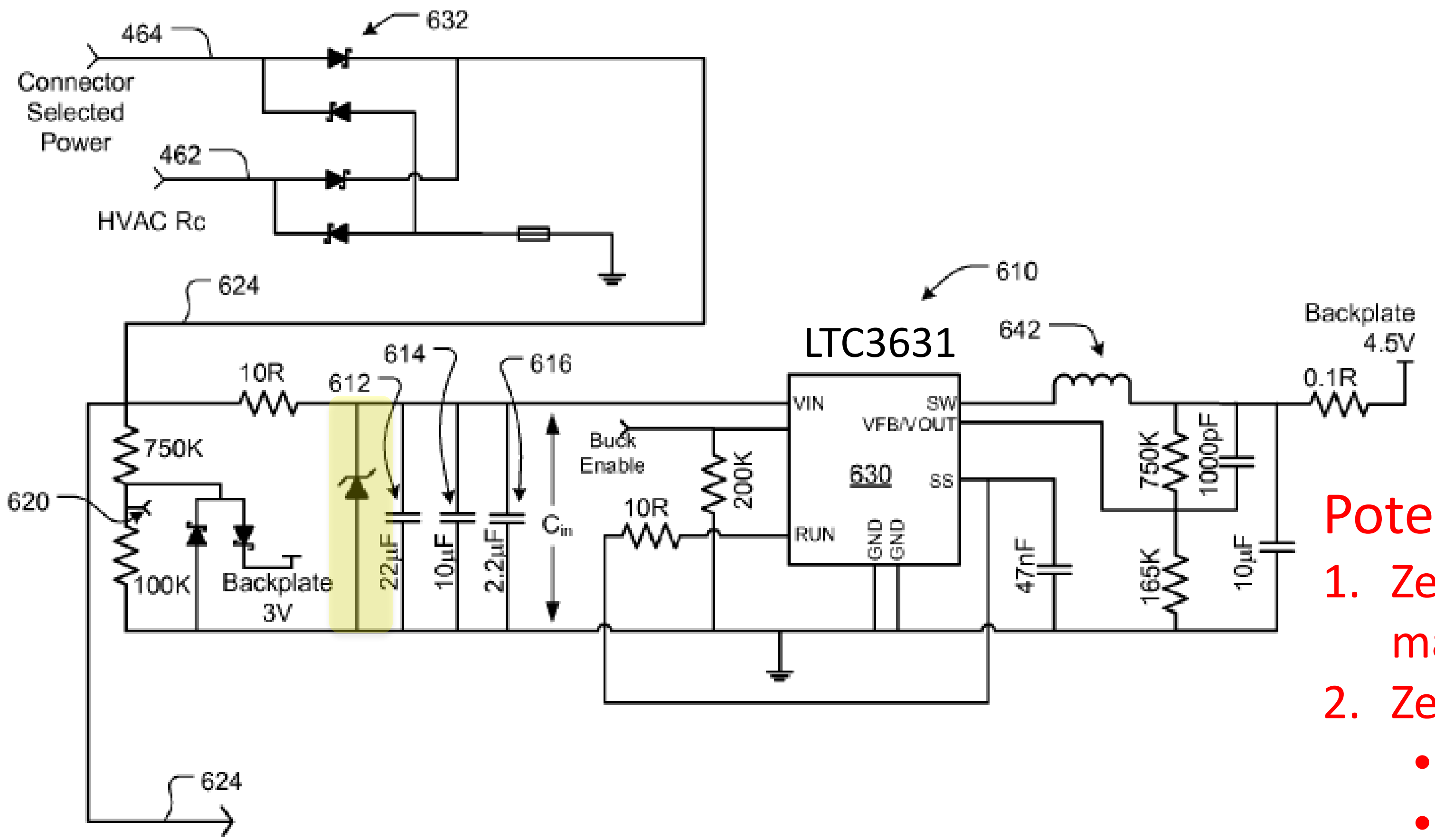
Potential failure modes and effects:

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

PURDUE
UNIVERSITY

FMECA ANALYSIS

High Voltage Buck Converter



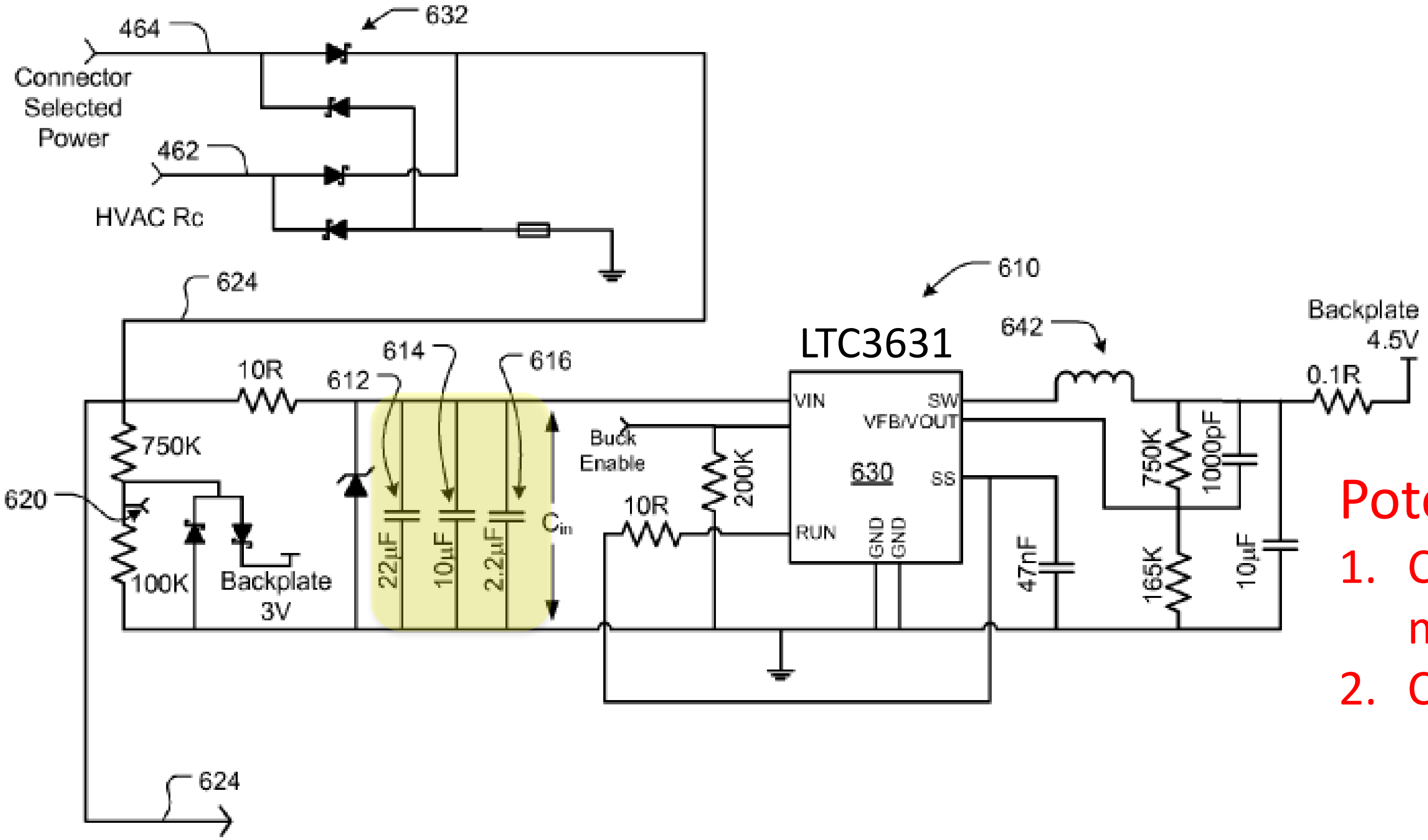
Potential failure modes and effects:

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

PURDUE
UNIVERSITY

FMECA ANALYSIS

High Voltage Buck Converter



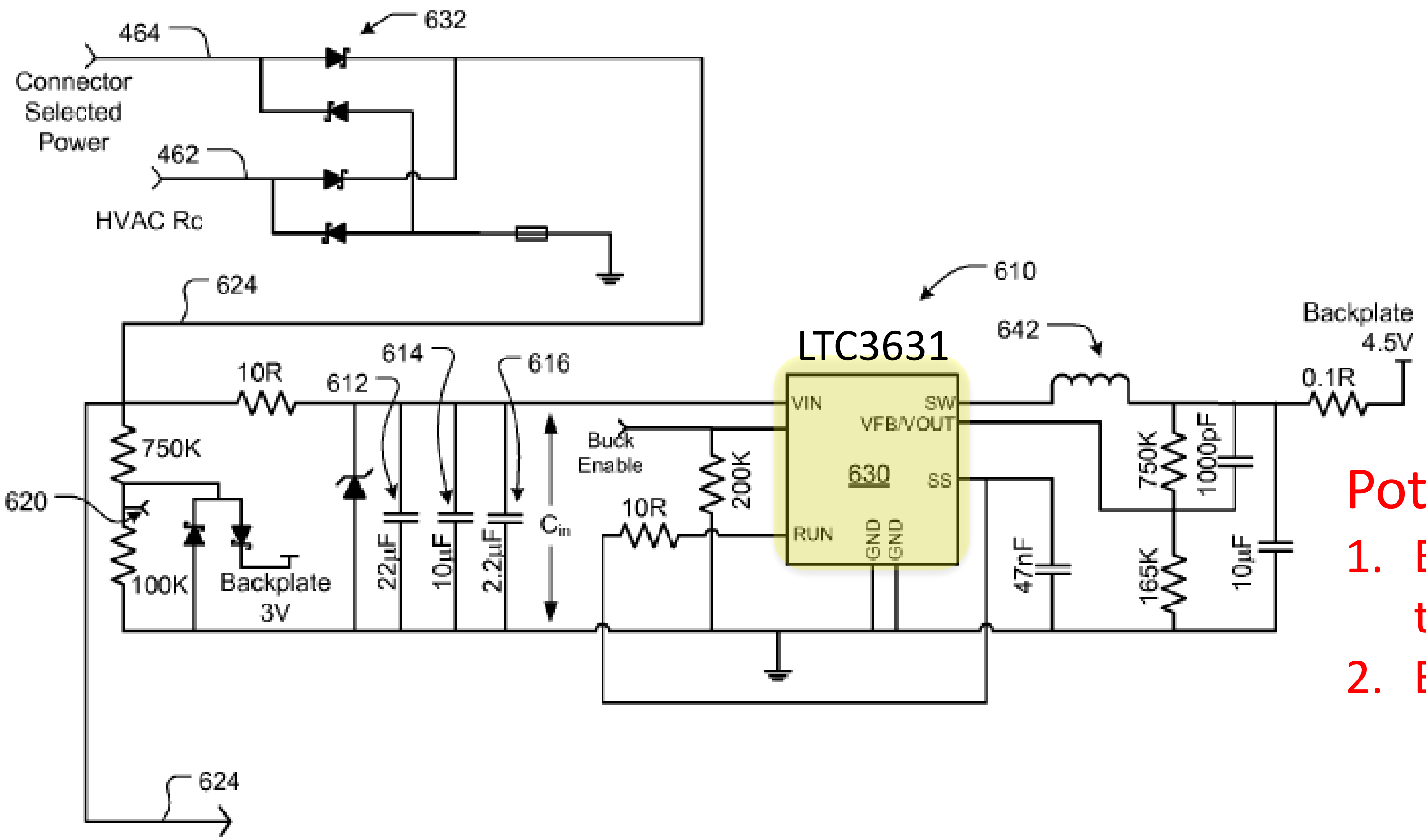
Potential failure modes and effects:

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

PURDUE
UNIVERSITY

FMECA ANALYSIS

High Voltage Buck Converter



Potential failure modes and effects:

1. Buck regulator fails with Vout = 0 → thermostat inoperative
2. Buck regulator fails with Vout = Vin
   - Overvoltage to backplate, fry most active components
   - Unpredictable effect on thermostat control contacts

PURDUE UNIVERSITY

FMECA ANALYSIS

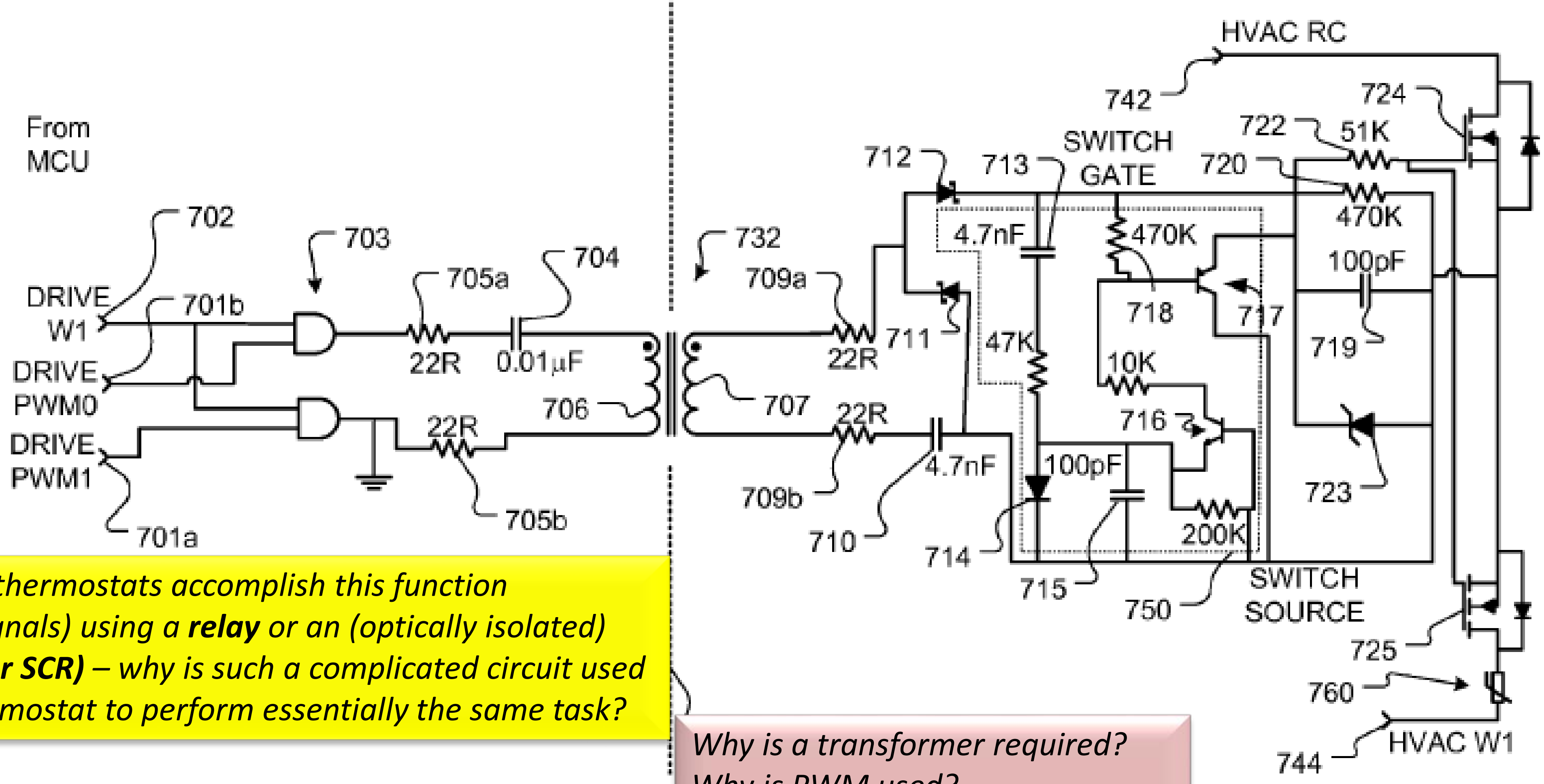
High Voltage Buck Converter

No.	Failure Mode	Possible Causes	Failure Effects	Detection Method	Criticality
1	Vout = 0	open PN diode failed regulator	unable to operate HVAC or charge battery	no current drawn from control contact	MEDIUM
2	Vout=0	shorted PN diode shorted capacitor shorted zener diode	HVAC stuck on, unable to charge battery	excessive current drawn from control contact	HIGH
3	Vout > 4.5	failed regulator	Unpredictable effect, potential for component damage	backplate supply voltage > 4.5 V	HIGH

PURDUE UNIVERSITY

FMECA ANALYSIS

Output Drive for Connection Between RC and W (or Y / G)



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?*

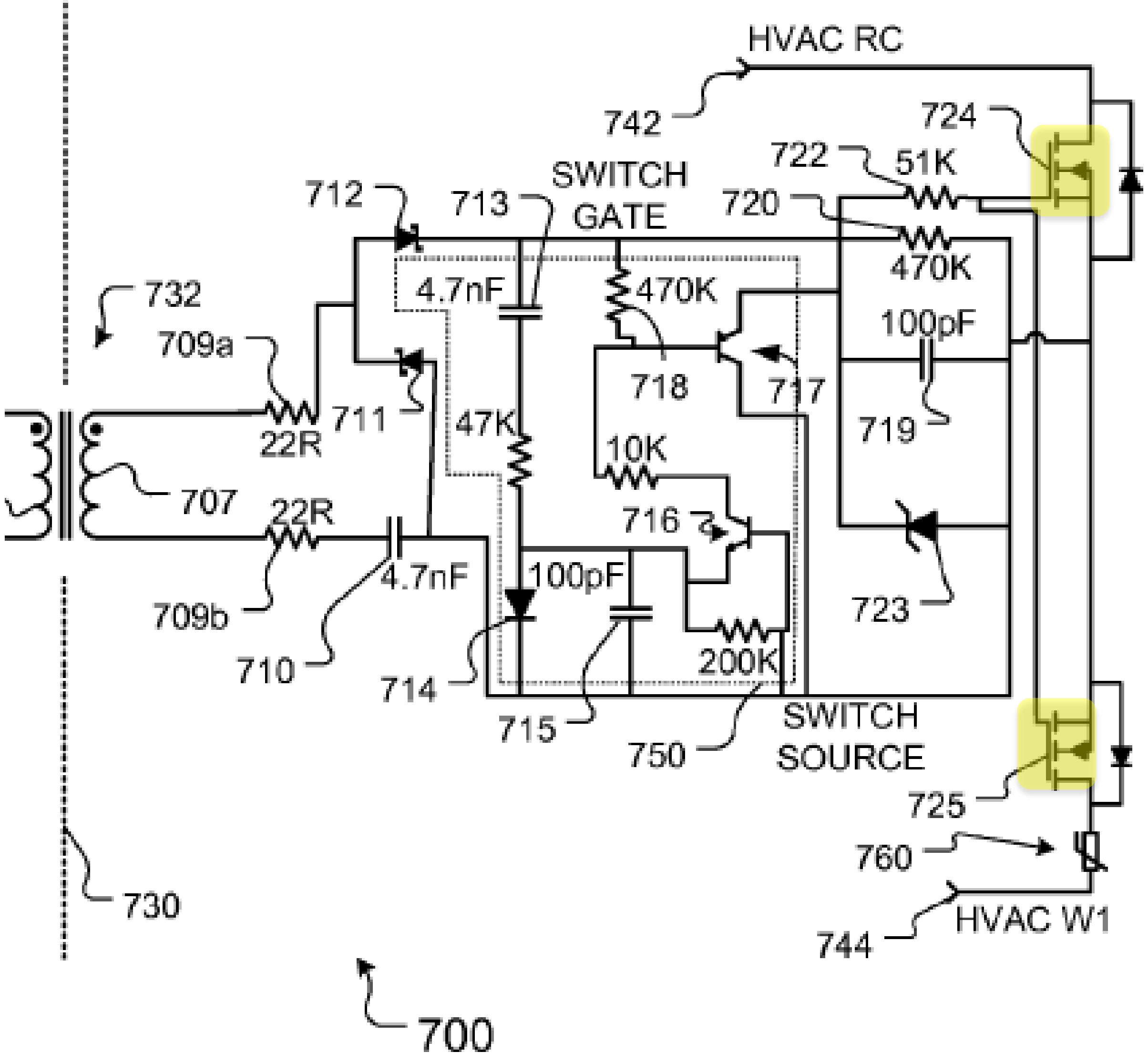
Why is a transformer required?
Why is PWM used?
Why are two MOSFETs required?

FMECA ANALYSIS

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



FMECA ANALYSIS

MOSFET Output Drive (Contact Closure)

No.	Failure Mode	Possible Causes	Failure Effects	Detection Method	Criticality
1	open	open MOSFET gate drive failed off	unable to operate HVAC	open (Hi-Z) control contact	MEDIUM
2	closed	shorted MOSFET gate drive failed on	HVAC stuck on, unable to charge battery	closed (shorted) control contact	HIGH
3	partial open	one MOSFET failed open	Unpredictable effect, may not be able to operate HVAC	“half-wave” control contact when ”on”	MEDIUM
4	partial closed	one MOSFET failed closed	Unpredictable effect, HVAC may be stuck on, battery charge current reduced	“half-wave” control contact when ”off”	HIGH

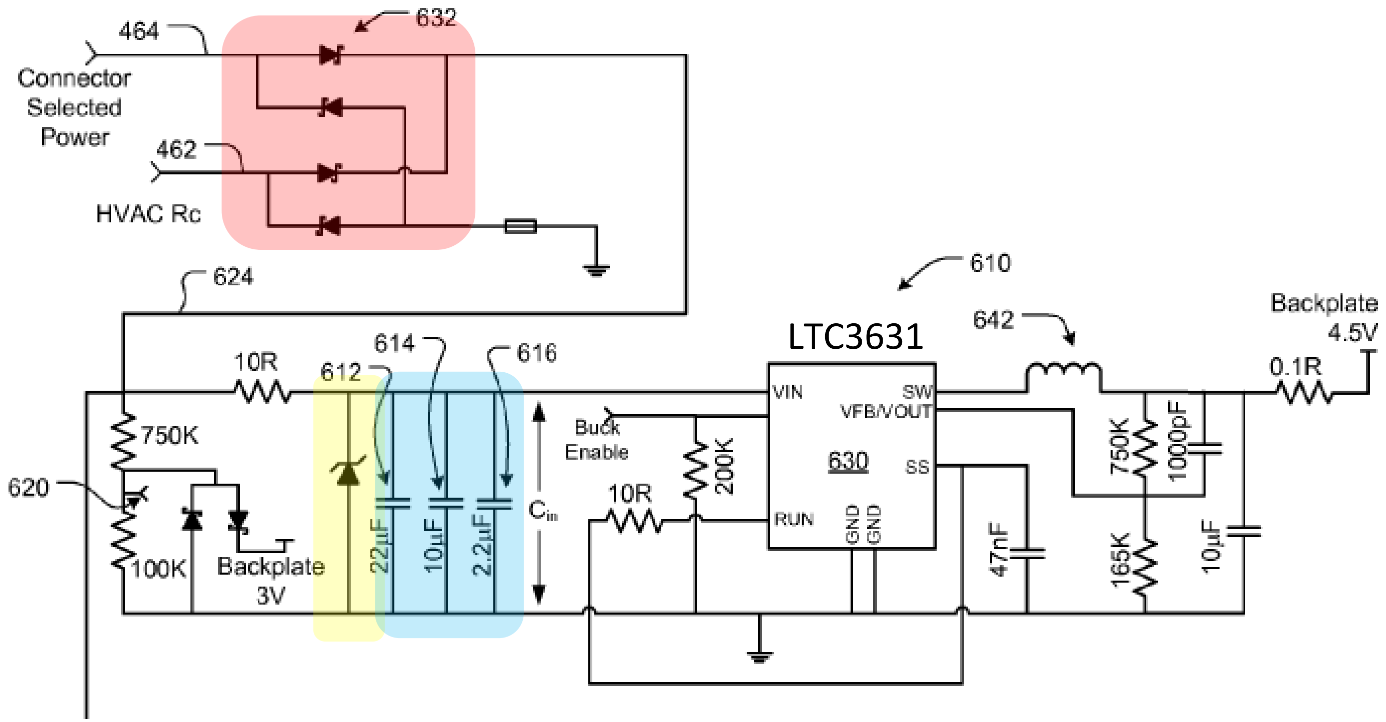
PURDUE UNIVERSITY

CLICKER QUIZ

Question 5

If <u>only one</u> of the PN junction diodes (highlighted in red) fails <u>open</u>, 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



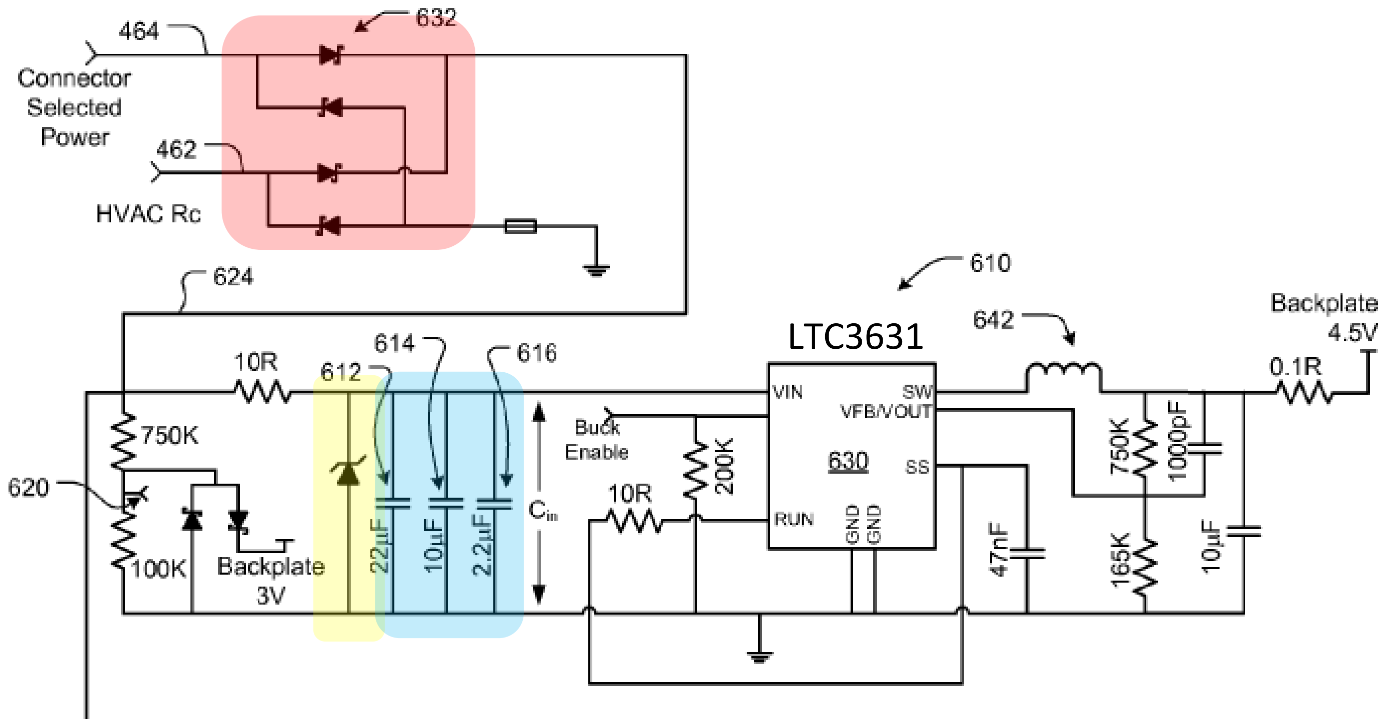
PURDUE UNIVERSITY

CLICKER QUIZ

Question 6

If the zener diode (highlighted in yellow) fails <u>open</u>, 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



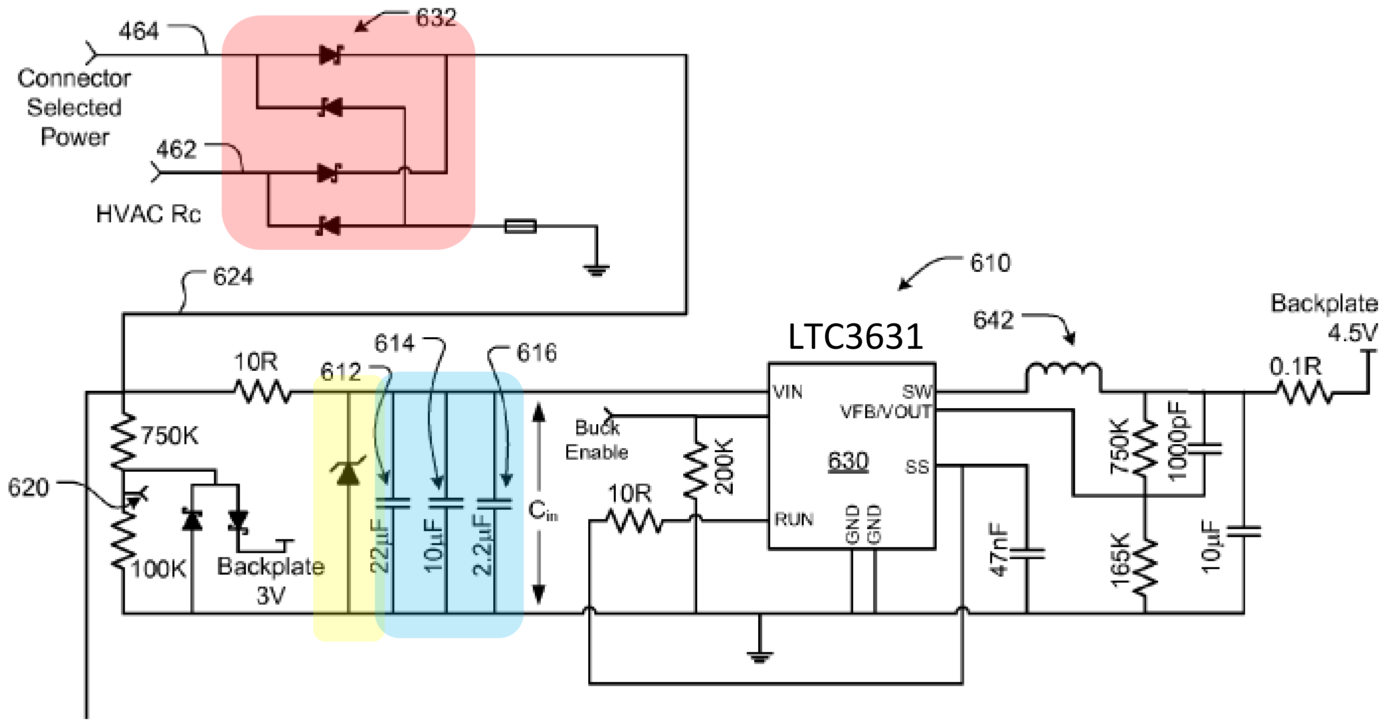
PURDUE UNIVERSITY

CLICKER QUIZ

Question 7

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



PURDUE UNIVERSITY

FAILURE REPORTS

Customer Complaints Documenting That Critical Failures Can and Do Occur

- *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 effecient Heil forced air gas furnace was "incompatable" 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 then the Nest's.*

PURDUE UNIVERSITY

RELIABILITY & SAFETY ANALYSIS REPORT

- 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 λ 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.*

PURDUE
UNIVERSITY

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.

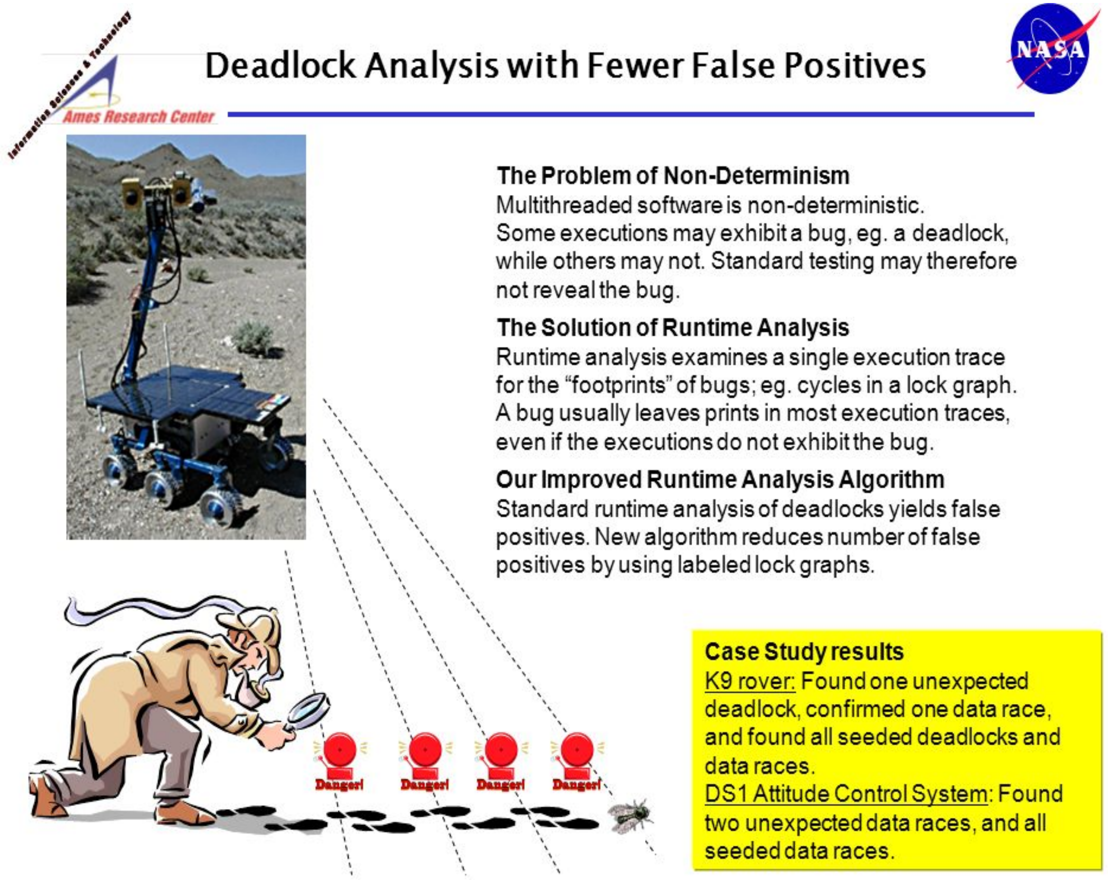
Temperature sensors
Three temperature sensors track your home's temperature and how quickly it changes.

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



PURDUE UNIVERSITY

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 ???*

PURDUE
UNIVERSITY

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)

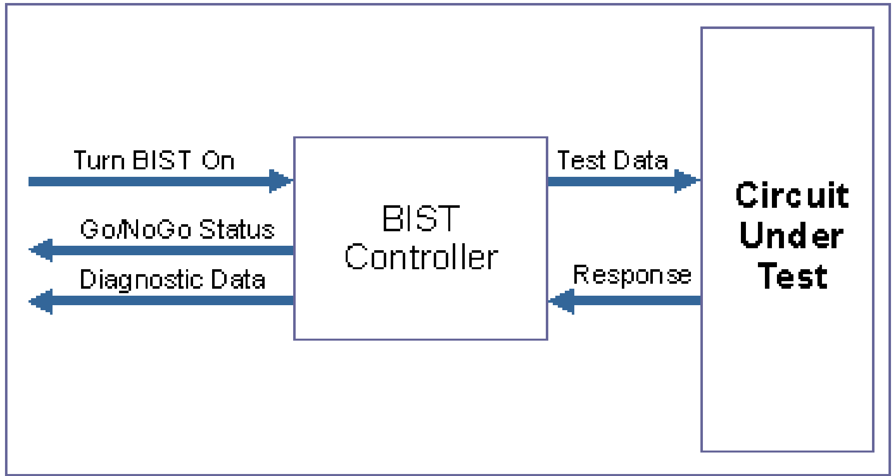


FIGURE 1. Autonomous BIST

PURDUE UNIVERSITY

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)

PURDUE
UNIVERSITY

STANDARDS AND COMPLIANCE

Example Category Relevant to ECE 477 Projects

IEC 62368-1 Audio/Video, Information and Communication Technology Equipment – Safety Requirements. Published Jan. 2010, UL & CSA versions, Feb. 2011

Arcade, Amusement and Gaming Machines – Bowling and Billiard Equipment – Cable and Satellite Communication Equipment – Circuit Components for Use in Audio/Video Equipment – Commercial Audio and Radio Equipment, Systems and Accessories – Low Voltage Portable Electronics; Household Audio and Video Equipment – Musical Instruments – Professional, Commercial and Household Use Equipment

PURDUE UNIVERSITY

STANDARDS AND COMPLIANCE

From ElectronicsDesign.com

The ABCs of IEC 62368-1, An Emerging Safety Standard (Posted: October 22, 2010)

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.

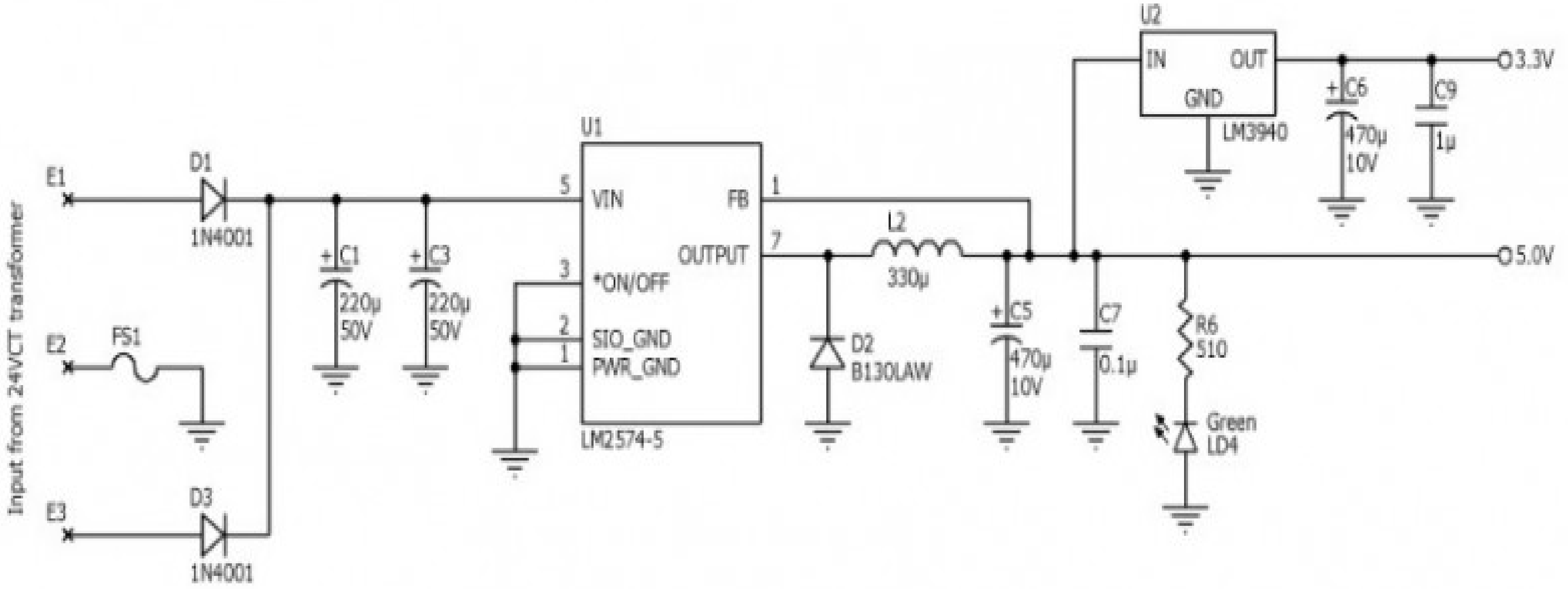
PURDUE UNIVERSITY

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



PURDUE UNIVERSITY

Source: *Circuit Cellar* April 2016 Electrical Engineering Challenge Circuit.