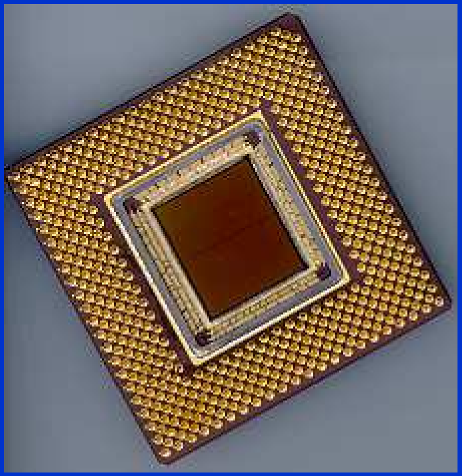
Spring 2014 Edition



ECE 477 Digital Systems Senior Design Project

Module 12

Designing for Reliability, Maintainability, and Safety

Outline

- **Introduction**
- **Component Failures and Wear**
- **Mean Time To/Before Failure (MTTF/MTBF)**
- **Heat Controller Example**
- **Failure Rate Calculation**
- **Improving System Availability**
- **Failure Mode & Effects Analysis (FMEA)**
- **Criticality Analysis (FMECA)**
- **Fault Tree Analysis (FTA)**
- **Software and Watchdogs**
- **Maintainability**
- **Standards and Compliance**

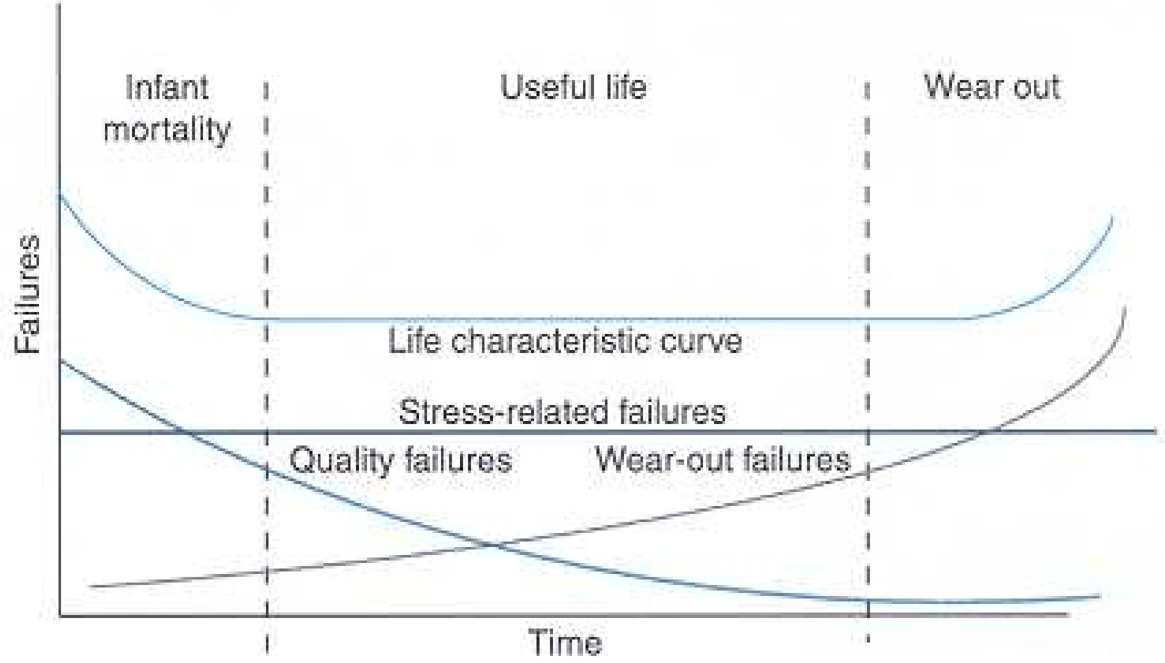
Reference: “Designing for Reliability, Maintainability, and Safety – Parts 1, 2, and 3”, Circuit Cellar, December 2000, January 2001, April 2001.

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, IEC, FCC standards (possibly others) to be met**

Component Failures

- 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



but…see May 2011 *IEEE Spectrum* feature article on “Transistor Aging”

Component Failures

- **Components do not “age” or “degrade” with use – constant failure rate unrelated to hours of use** *(under certain conditions)*
- **Equivalent information is gained testing10 units for 10,000 hours vs. testing 1000 units for 100 hours**
- **“Impossible” 10^{-9} failure as likely to happen in the first 5 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 unit failures per million hours, i.e., [10^{-6} units/hr) (given just one unit is involved)**
- **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 × unit)]**
- **Equivalent to:**
  - **number of failures per unit per million hours**
  - **number of failures/hour given 1 million units in field (assuming failed units are replaced)**

Definition of Failure Rate

- **Given $\lambda_p \times 10^{-6}$ [fails/(hr × 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 × unit) × N units × 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 × unit) × 1000 units × (365 × 24) hours = 17.52**

Definition of Failure Rate

- Given $\lambda_p \times 10^{-6}$ [fails/(hr × 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 × unit) × N units × 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 × 7 × 24 hrs) = 0.595×10^{-6} failures per unit per hour**

Clicker Quiz

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 x 10^{-6} units/hr, should you be “happy” if a if a typical single unit only fails once in 114 years on average ?

   A. **yes**

   B. **no**

3. How long between unit failures will it be if you have 1 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 this failure causes serious injury?
   - A. **yes**
   - B. **no**

Component Wear*

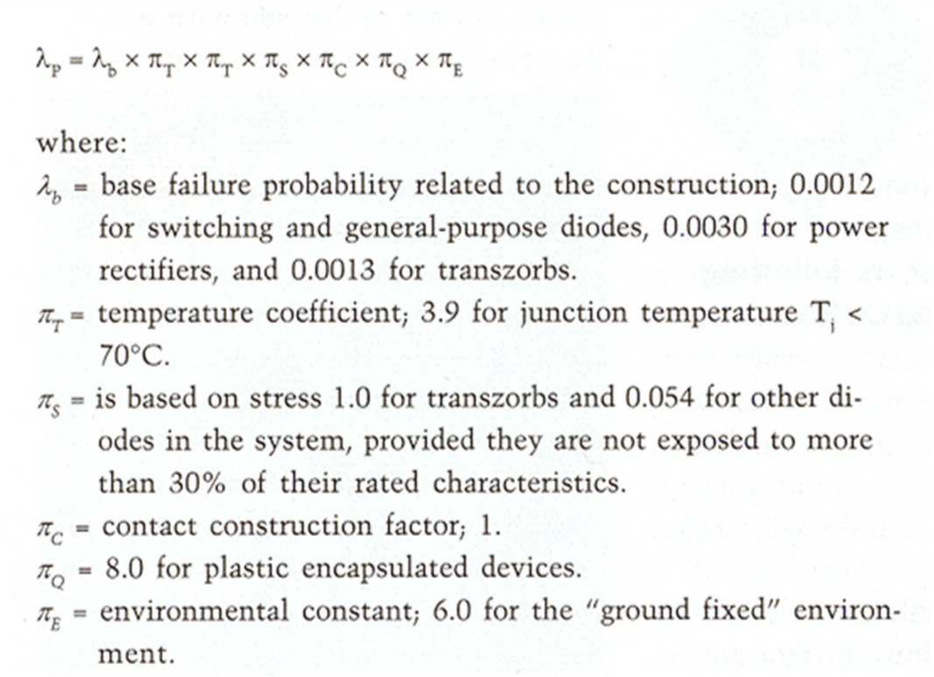
- **If, based on observation, failure rate does depend on time used, it may be due to wear caused by *improper derating***
- **Well-derated electronic systems seldom reach the point of wear-out failure**
- **Well-derated = working at < 30-40% of specified ratings**
- **Heat is the main reliability killer – even a small reduction will have a significant effect**

***See also "An Odometer for CPUs," *IEEE Spectrum*, May 2011**

Reliability Models for Components

- Calculated value is λ_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:

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.

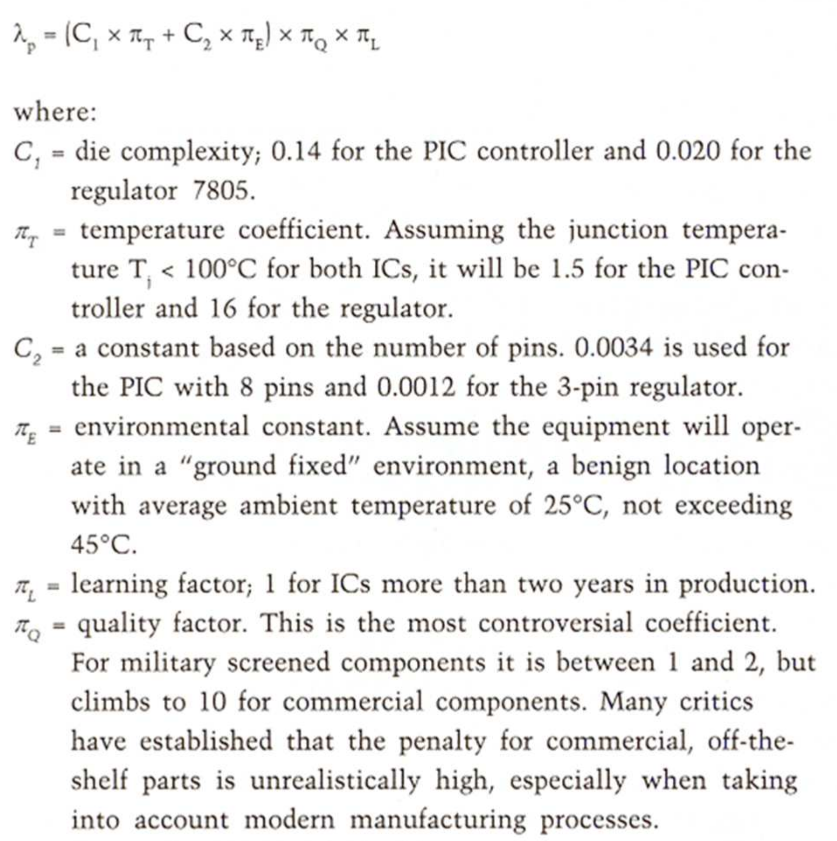
π_S = is based on stress 1.0 for transzorbs and 0.054 for other diodes in the system, provided they are not exposed to more than 30% of their rated characteristics.

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.

Microelectronic Circuits



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

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.

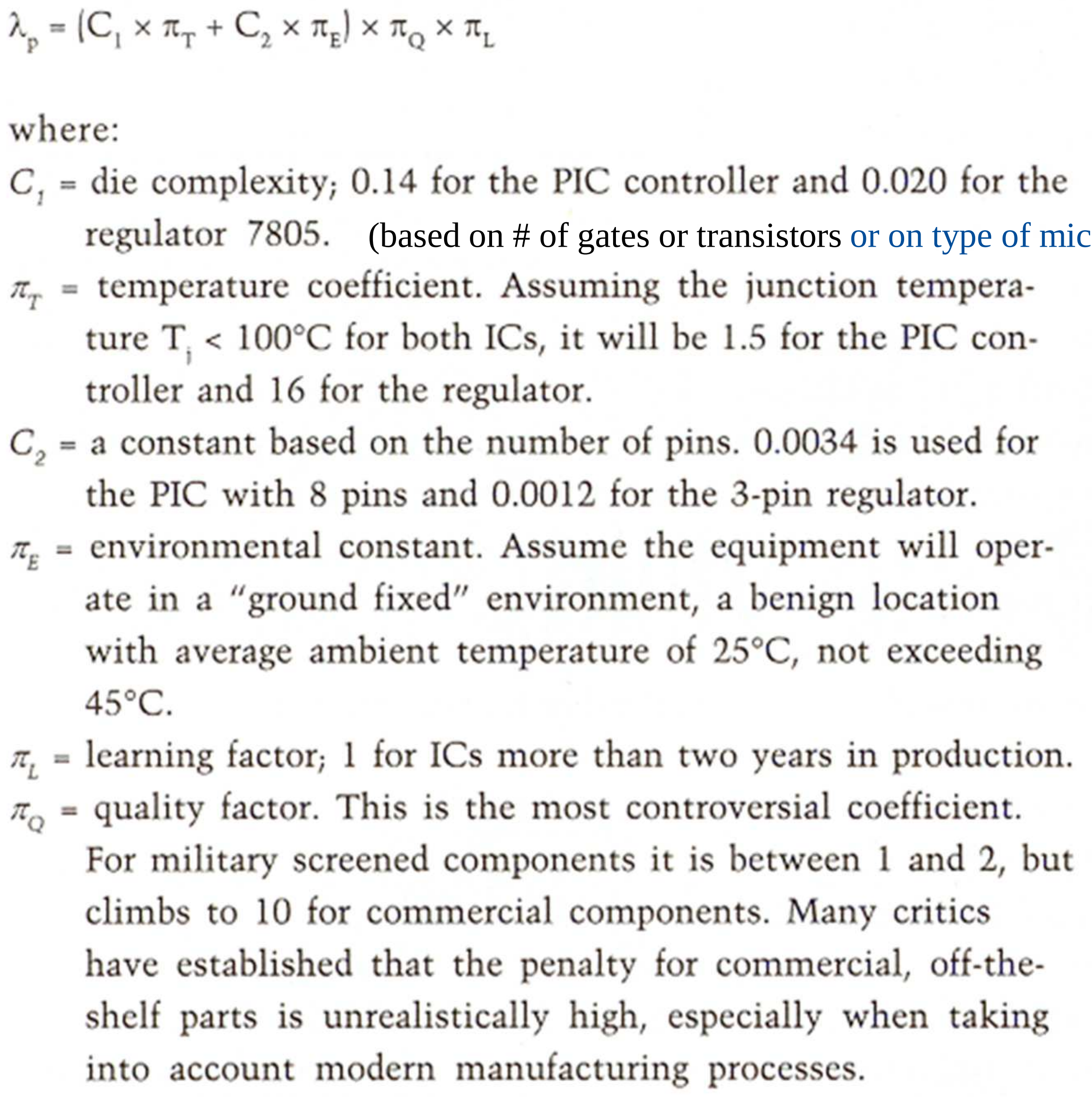
C_2 = a constant based on the number of pins. 0.0034 is used for the PIC with 8 pins and 0.0012 for the 3-pin regulator.

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.

Microelectronic Circuits (see 5.1 p.23ff of Mil-Hdbk 217F)



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

where:

C_1 = die complexity; 0.14 for the PIC controller and 0.020 for the regulator 7805. (based on # of gates or transistors or on type of micro, e.g., 8bit, 16bit, etc)

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.

Expectations for Homework

- Choose hottest and/or most complex components
  - Which are your hottest/most complex components?
- Choose most closely related MIL-HDBK-217F model
- List assumptions and rationale for parameter values used
- Present information as table or bullet list

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)

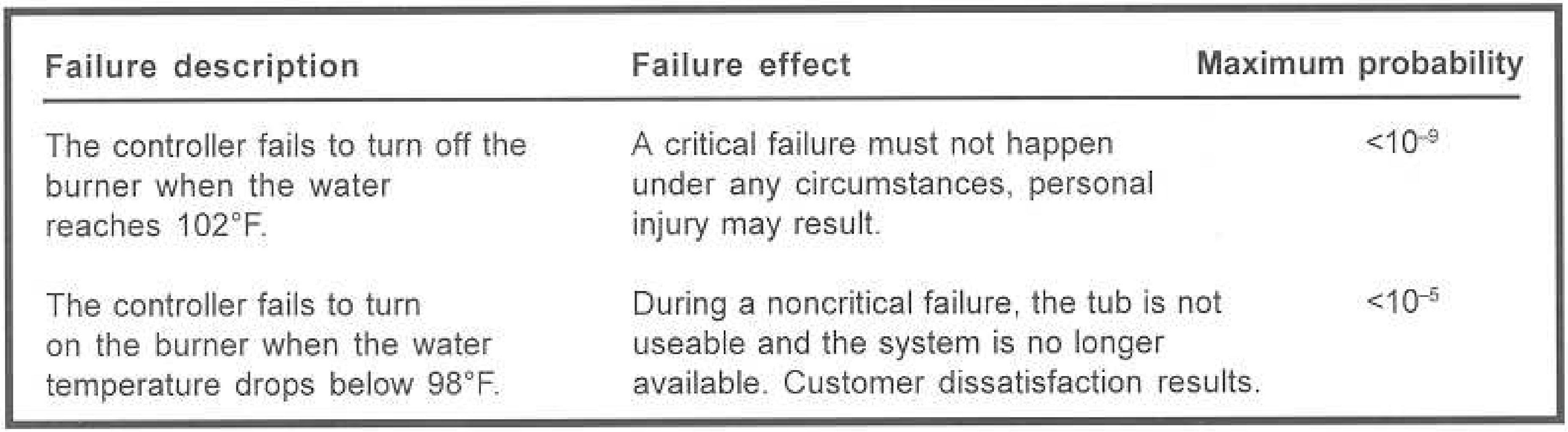
Heat Controller Example

- Gas-fired burner to maintain hot-tub water temperature within a specified tolerance
- Possibility of personal injury if controller malfunctions
- Performing hazard analysis and modifying the design based on results obtained
  - important for showing “reasonable care” in court (reduction of liability)

Heat Controller Example

- **Simple hazard analysis**
- **10^{-9} generally accepted as "never"**
  (50% chance of failure after 79,000 years of continuous operation)

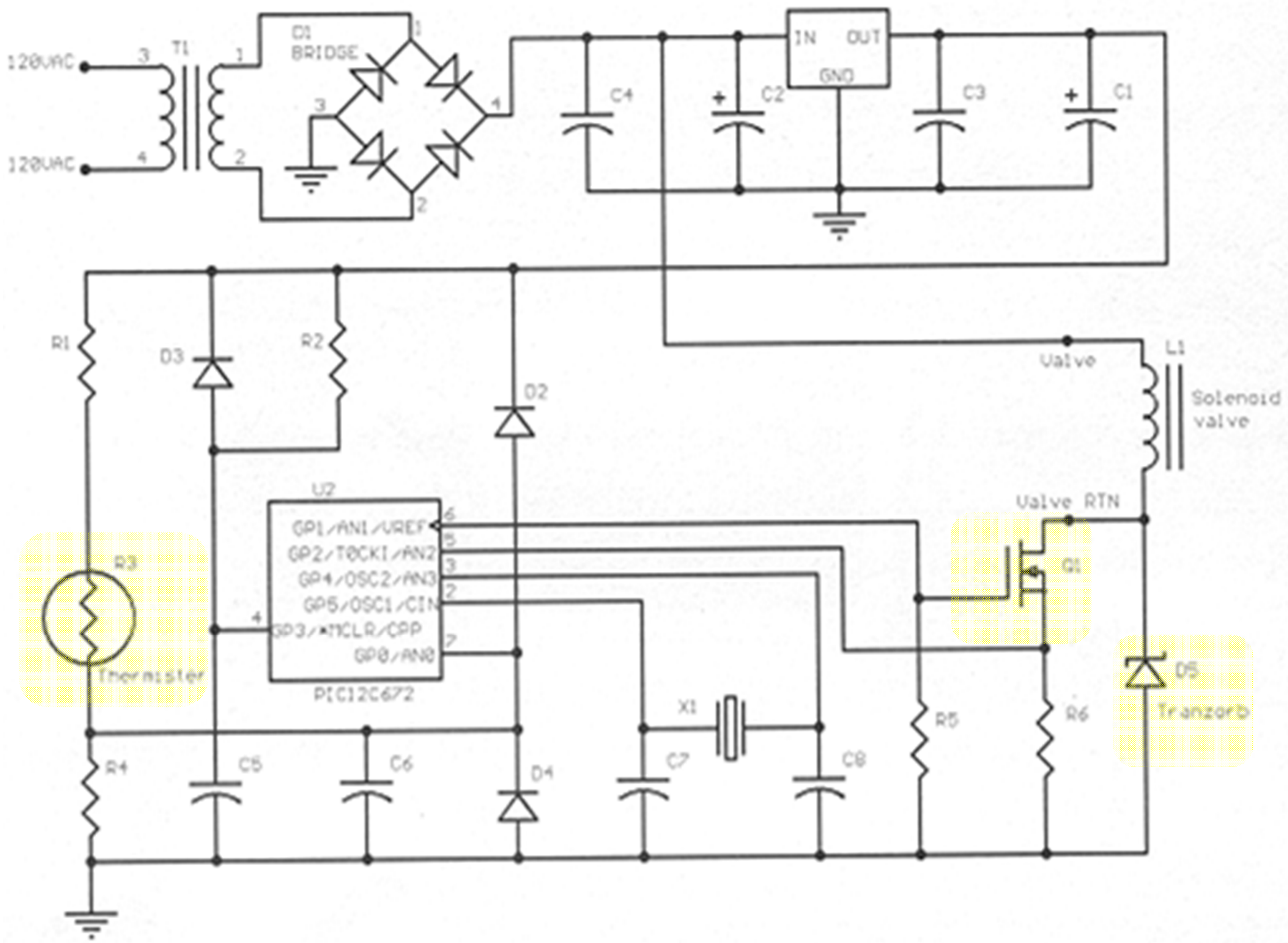
  BTW: with 1M units in field**, <u>never</u>** occurs once every 6 weeks



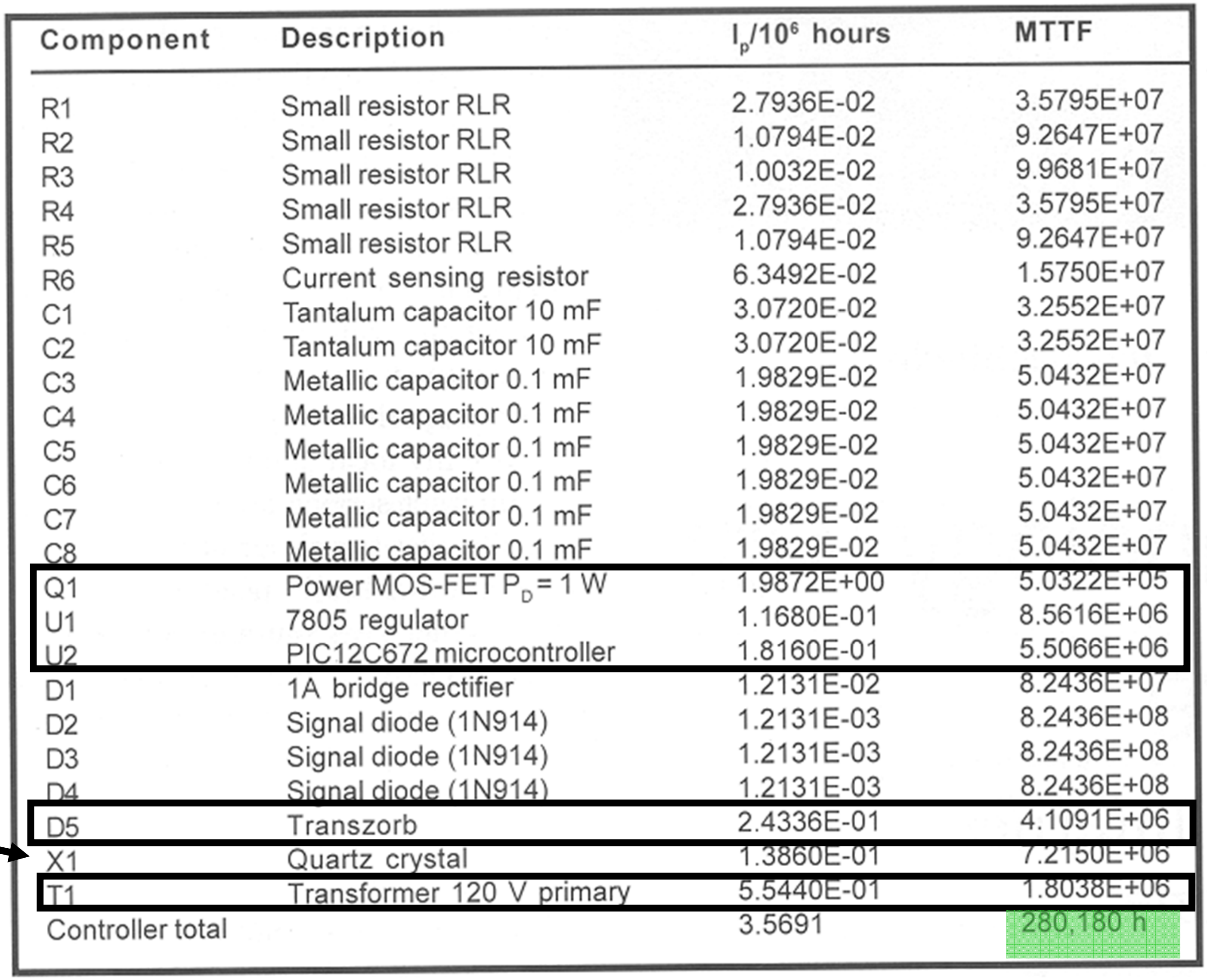
Failure description	Failure effect	Maximum probability
The controller fails to turn off the burner when the water reaches 102°F.	A critical failure must not happen under any circumstances, personal injury may result.	$<10^{-9}$
The controller fails to turn on the burner when the water temperature drops below 98°F.	During a noncritical failure, the tub is not useable and the system is no longer available. Customer dissatisfaction results.	$<10^{-5}$

Initial Circuit Design

What is the purpose of R3, Q1, and D5?



Preliminary Failure Rate Calculation



Component	Description	$l_p/10^6$ hours	MTTF
R1	Small resistor RLR	2.7936E-02	3.5795E+07
R2	Small resistor RLR	1.0794E-02	9.2647E+07
R3	Small resistor RLR	1.0032E-02	9.9681E+07
R4	Small resistor RLR	2.7936E-02	3.5795E+07
R5	Small resistor RLR	1.0794E-02	9.2647E+07
R6	Current sensing resistor	6.3492E-02	1.5750E+07
C1	Tantalum capacitor 10 mF	3.0720E-02	3.2552E+07
C2	Tantalum capacitor 10 mF	3.0720E-02	3.2552E+07
C3	Metallic capacitor 0.1 mF	1.9829E-02	5.0432E+07
C4	Metallic capacitor 0.1 mF	1.9829E-02	5.0432E+07
C5	Metallic capacitor 0.1 mF	1.9829E-02	5.0432E+07
C6	Metallic capacitor 0.1 mF	1.9829E-02	5.0432E+07
C7	Metallic capacitor 0.1 mF	1.9829E-02	5.0432E+07
C8	Metallic capacitor 0.1 mF	1.9829E-02	5.0432E+07
Q1	Power MOS-FET P_D = 1 W	1.9872E+00	5.0322E+05
U1	7805 regulator	1.1680E-01	8.5616E+06
U2	PIC12C672 microcontroller	1.8160E-01	5.5066E+06
D1	1A bridge rectifier	1.2131E-02	8.2436E+07
D2	Signal diode (1N914)	1.2131E-03	8.2436E+08
D3	Signal diode (1N914)	1.2131E-03	8.2436E+08
D4	Signal diode (1N914)	1.2131E-03	8.2436E+08
D5	Transzorb	2.4336E-01	4.1091E+06
X1	Quartz crystal	1.3860E-01	7.2150E+06
T1	Transformer 120 V primary	5.5440E-01	1.8038E+06
Controller total		3.5691	280,180 h

Improving System Availability

- **Components with greater failure rates than the rest (Q1, U1, U2, D5, T1, X1)**
- **Q1, U1, U2 work at conservatively estimated junction temperature of 100°C**
  - – efficient heat sinking can reduce junction temperature to 50ºC ($\Delta T = P_{diss} \times R_{th}$) $T = T_{ambient} + \Delta T$
- **Transzorb D5 & diodes D2, D3 conduct during infrequent transients only**
  - – reduce their contribution by applying a duty cycle
- **Design T1 to run at a lower temperature to improve its reliability**

Improving System Availability

- Implementing these steps
  - Increase MTBF from 280,000 hours to 714,000 hr.
  - λ_p = 1.4 [failures/10^6 hours]
- For the remaining analysis (Part 2), the results of these calculations will be used to evaluate and improve product safety

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)**

FMEA

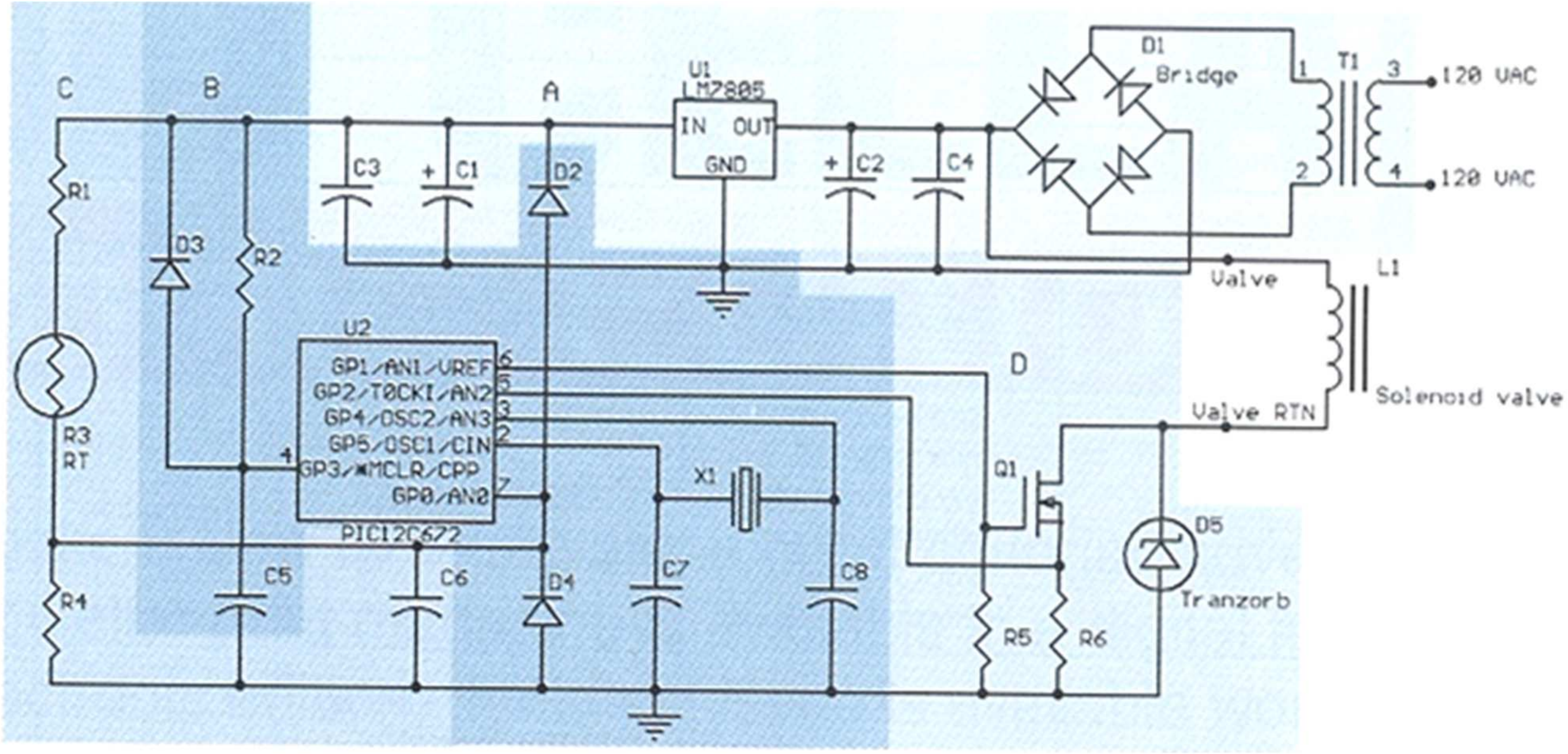
- Bottom-up review of a system
- Examine components for failure modes
- Note how failures propagate through system
- Study effects on system behavior
- Leads to design review and possibly changes to eliminate weaknesses

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*

* probability calculation not required for homework

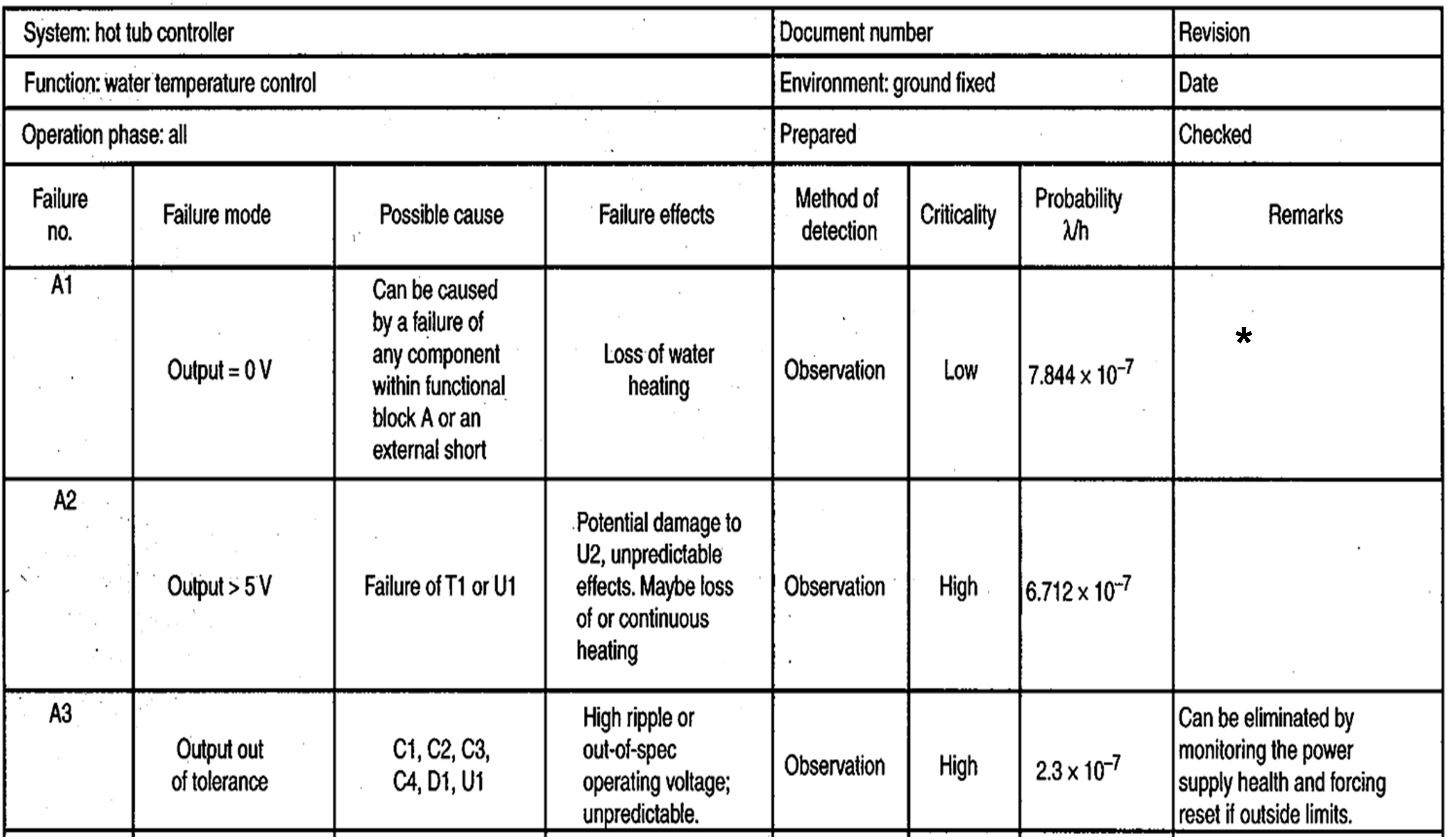
Original Circuit



What would be the effect of a failure of R3, Q1, or D5?

(what if they fail open? shorted?)

Power supply



System: hot tub controller	Document number	Revision
Function: water temperature control	Environment: ground fixed	Date
Operation phase: all	Prepared	Checked

Failure no.	Failure mode	Possible cause	Failure effects	Method of detection	Criticality	Probability λ/h	Remarks
A1	Output = 0 V	Can be caused by a failure of any component within functional block A or an external short	Loss of water heating	Observation	Low	7.844×10^{-7}	*
A2	Output > 5 V	Failure of T1 or U1	Potential damage to U2, unpredictable effects. Maybe loss of or continuous heating	Observation	High	6.712×10^{-7}	
A3	Output out of tolerance	C1, C2, C3, C4, D1, U1	High ripple or out-of-spec operating voltage; unpredictable.	Observation	High	2.3×10^{-7}	Can be eliminated by monitoring the power supply health and forcing reset if outside limits.

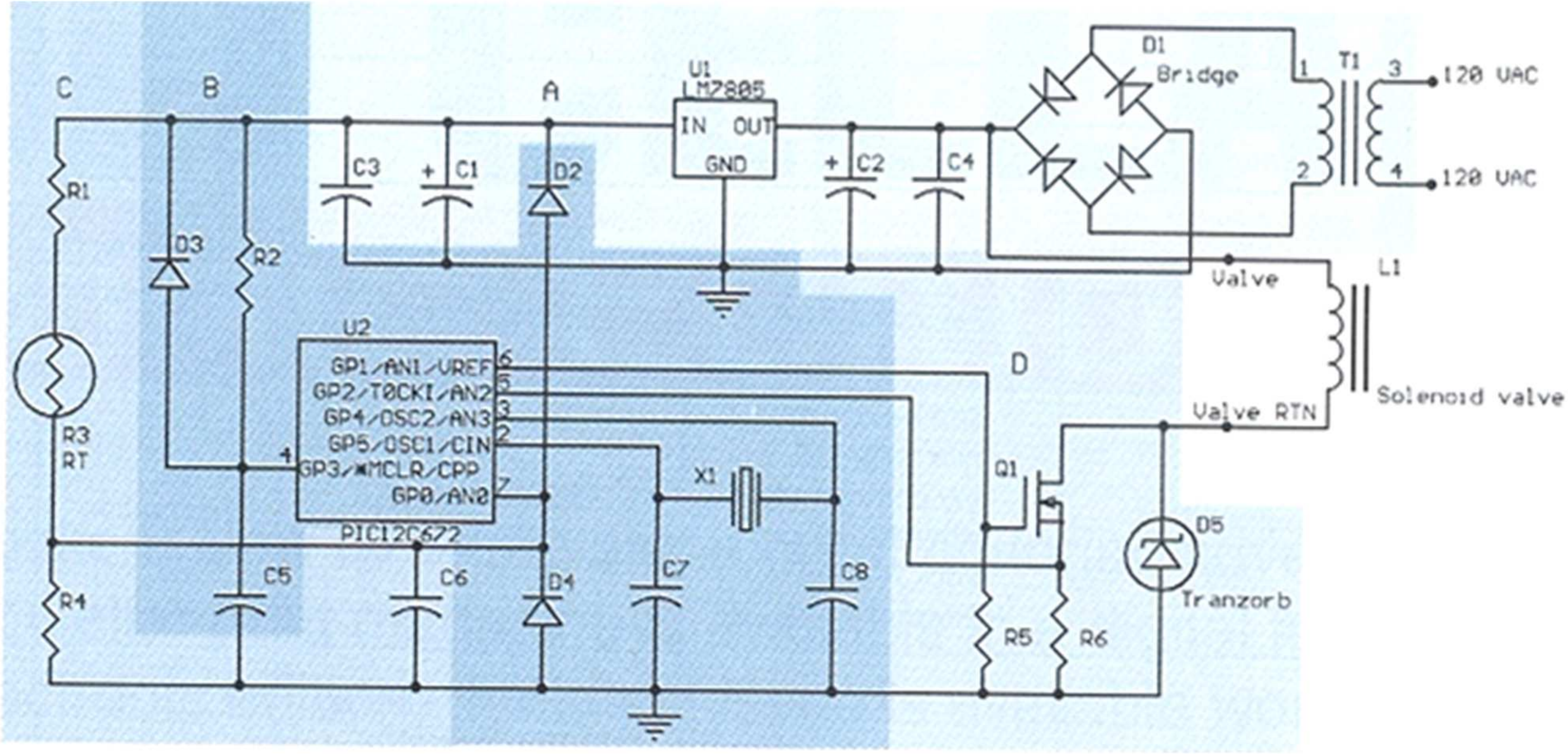
Note: some causes of 0 V could be overheat, fire, or chemical hazard, could then be a critical failure.

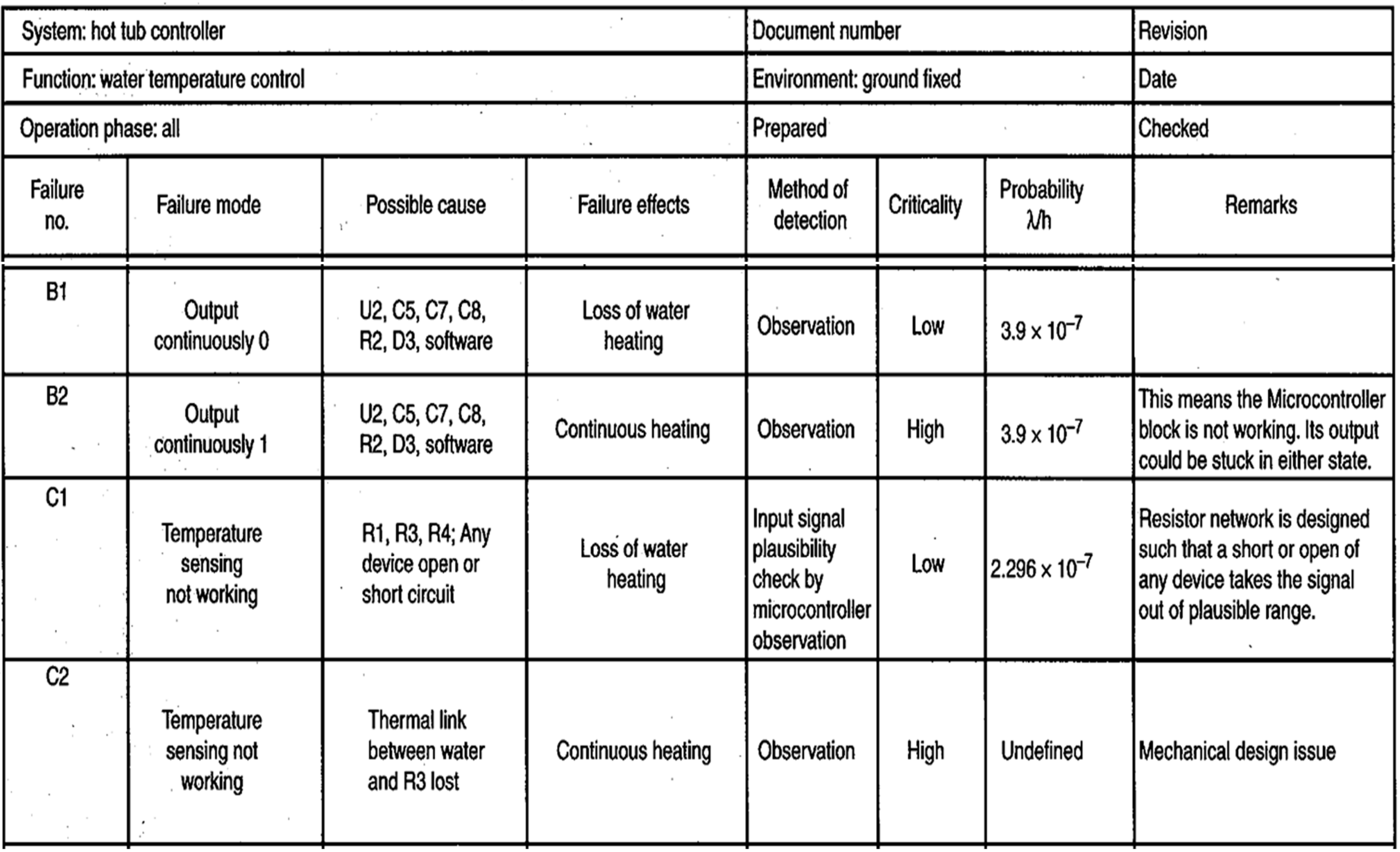
Failure Cause/Mode/Effect/Criticality

(use Circuit Cellar 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 hot tub, it either overheats or under-heats the water
  - 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 ≤ 10^{-9} _
  - Medium (optional): _renders system unrepairable________________
  - Low: _inconvenience to user, required rate typically > 10^{-6}_______

Original Circuit



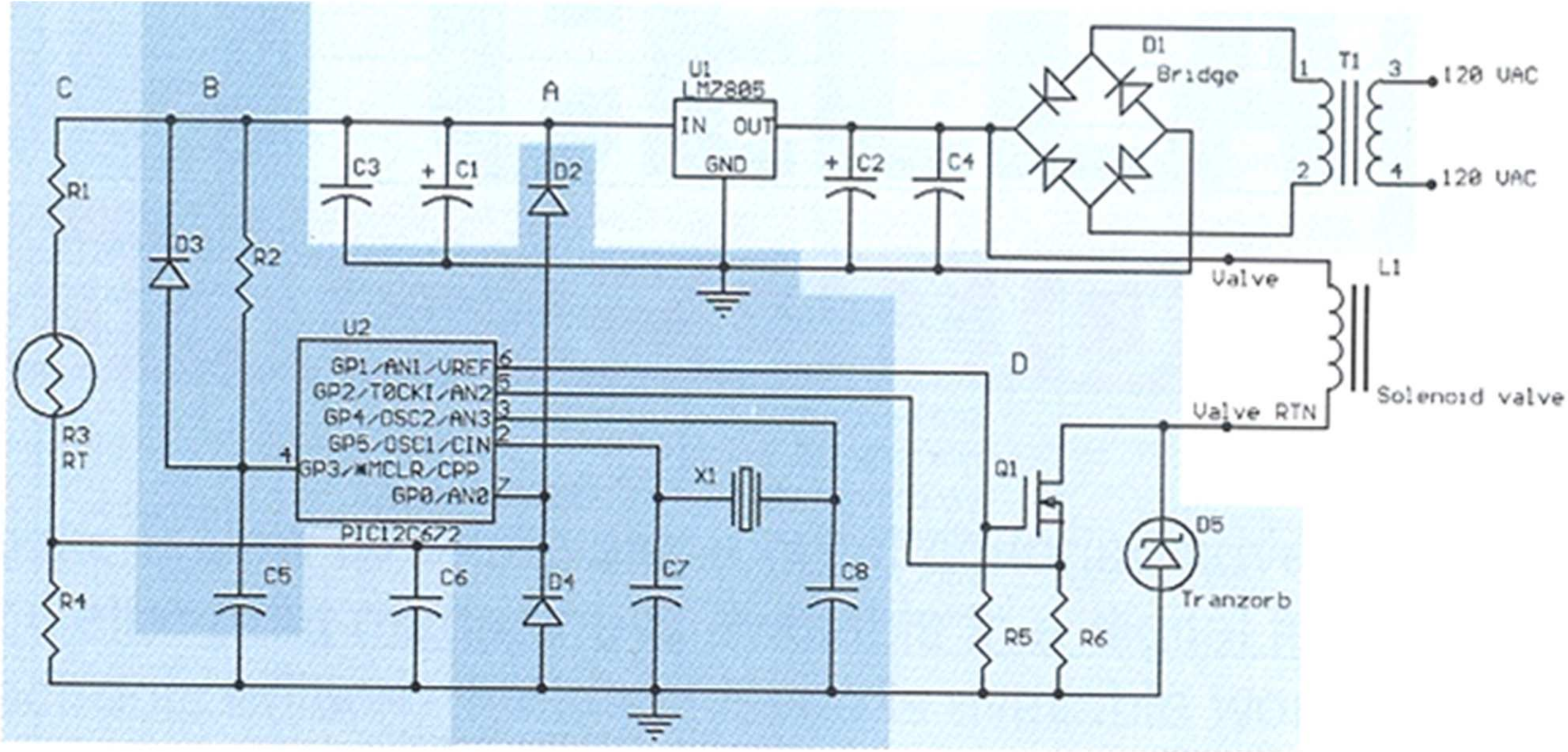


System: hot tub controller				Document number			Revision
Function: water temperature control				Environment: ground fixed			Date
Operation phase: all				Prepared			Checked
Failure no.	Failure mode	Possible cause	Failure effects	Method of detection	Criticality	Probability λ/h	Remarks
B1	Output continuously 0	U2, C5, C7, C8, R2, D3, software	Loss of water heating	Observation	Low	3.9×10^{-7}	
B2	Output continuously 1	U2, C5, C7, C8, R2, D3, software	Continuous heating	Observation	High	3.9×10^{-7}	This means the Microcontroller block is not working. Its output could be stuck in either state.
C1	Temperature sensing not working	R1, R3, R4; Any device open or short circuit	Loss of water heating	Input signal plausibility check by microcontroller observation	Low	2.296×10^{-7}	Resistor network is designed such that a short or open of any device takes the signal out of plausible range.
C2	Temperature sensing not working	Thermal link between water and R3 lost	Continuous heating	Observation	High	Undefined	Mechanical design issue

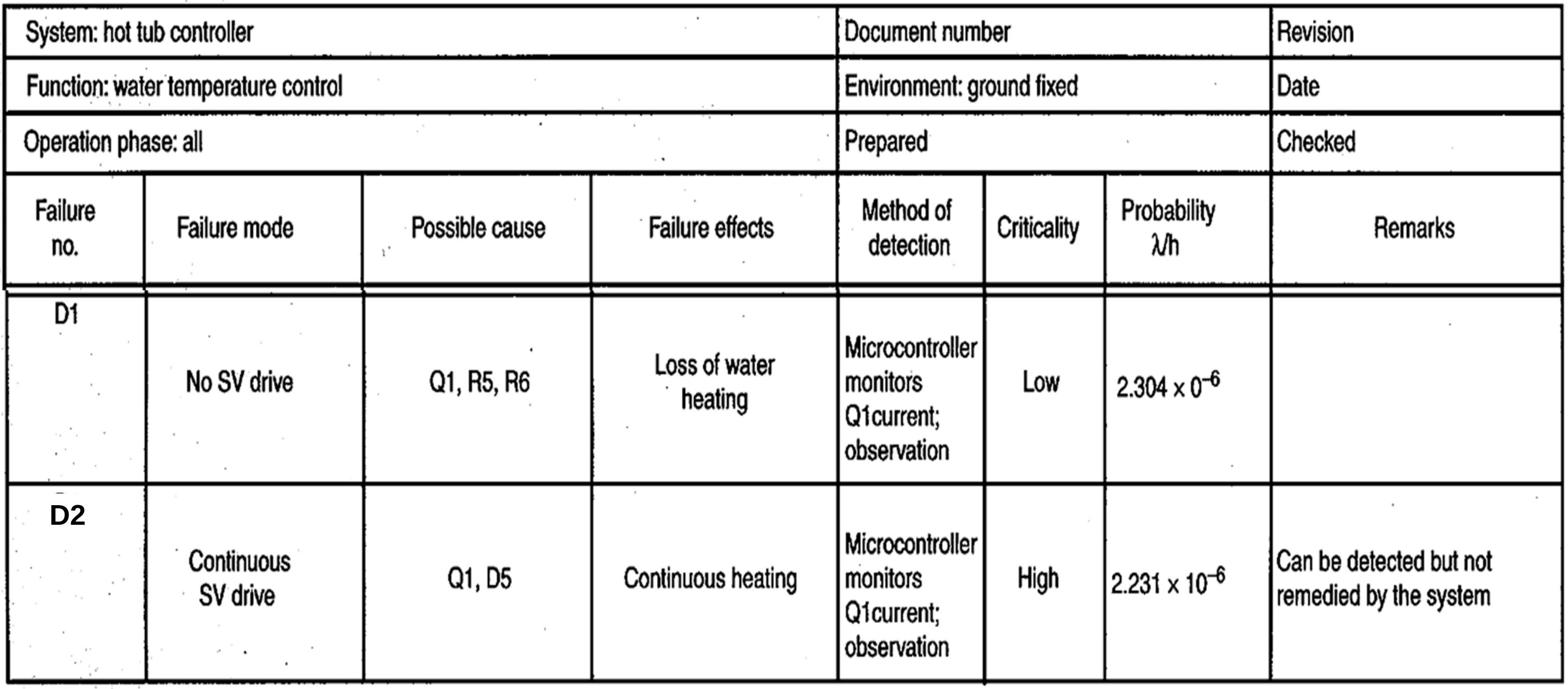
micro

temp. sense

Original Circuit



solenoid drive



System: hot tub controller				Document number			Revision
Function: water temperature control				Environment: ground fixed			Date
Operation phase: all				Prepared			Checked
Failure no.	Failure mode	Possible cause	Failure effects	Method of detection	Criticality	Probability λ/h	Remarks
D1	No SV drive	Q1, R5, R6	Loss of water heating	Microcontroller monitors Q1current; observation	Low	2.304×0^{-6}	
D2	Continuous SV drive	Q1, D5	Continuous heating	Microcontroller monitors Q1current; observation	High	2.231×10^{-6}	Can be detected but not remedied by the system

High Criticality Failures

- **A2 – power supply over-voltage**
- **A3 – power supply out of tolerance (too high or too low)**
- **B2 – micro failure or software malfunction**
- **C2 – temperature sensor**
- **D2 – solenoid drive**

In Class Team Exercise

Part 1: Define criticality levels for your project

(a) **low**

(b) **medium**

(c) **high**

Part 2: Identify one potential high criticality failure mode

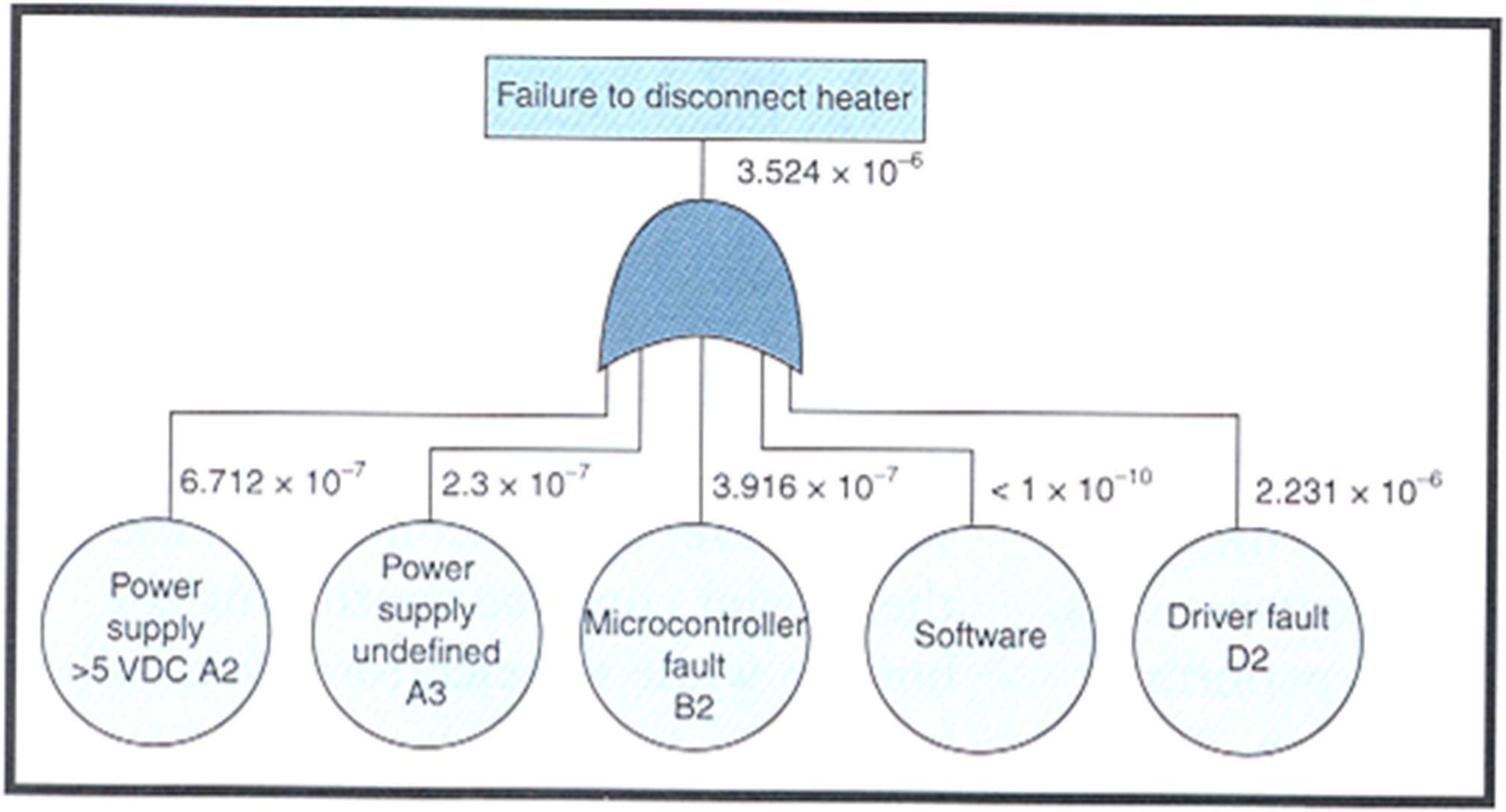
(a) **descriptive name**

(b) **potential cause**

(c) **effect**

Fault Tree Analysis (FTA)

- **Purpose:** estimate probability of a particular failure mode or set of failure modes
- **Top-down graphical analysis**
- **Starts with top event of interest**
- **Builds fault tree using Boolean logic and symbols**
- **Incorporating known failure probabilities (same as used in FMECA) yields probability of event of interest**
  - OR probabilities added (accurate only for small probabilities)
  - AND probabilities multiplied


Failure to disconnect heater
3.524 × 10^-6
6.712 × 10^-7
2.3 × 10^-7
3.916 × 10^-7
< 1 × 10^-10
2.231 × 10^-6
Power supply >5 VDC A2
Power supply undefined A3
Microcontroller fault B2
Software
Driver fault D2

Probability of Failure

$P_F = 1 - e^{-\lambda t}$

note: for small t, $P_F \cong \lambda$

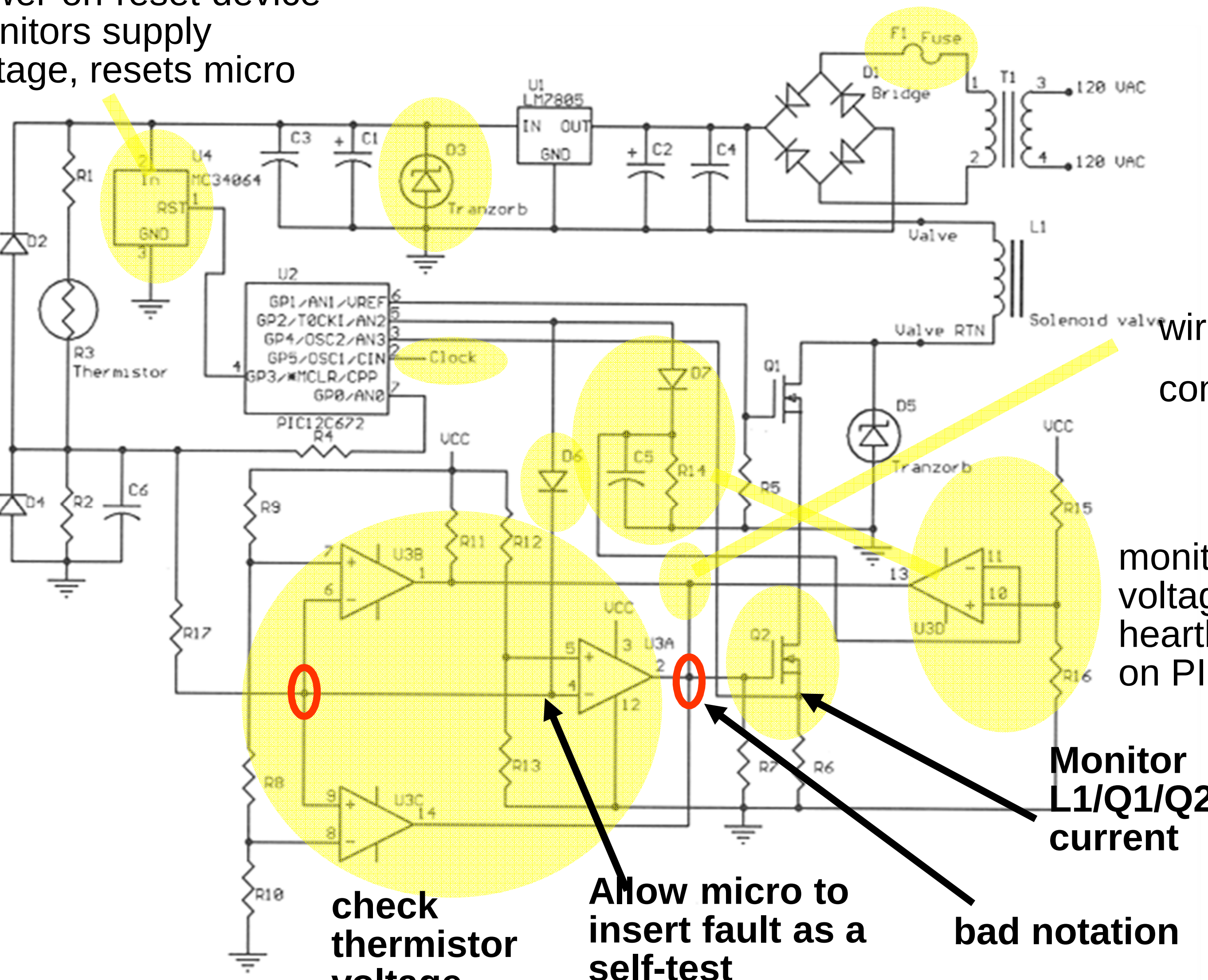
For $P_F = 0.5$ (50% chance of uncontrolled heating), **it takes 22 years of operation given** $\lambda = 3.5424 \times 10^{-6}$

NOT GOOD ENOUGH FOR A SYSTEM THAT CAN POTENTIALLY CAUSE INJURY – NEED $\lambda = 10^{-9}$

(78,767 years for $P_F = 50\%$)

Adding Hardware Monitors

(and monitors for the hardware monitors)



power-on-reset device monitors supply voltage, resets micro

wired OR of

comparators

monitor C5 voltage as a heartbeat check on PIC

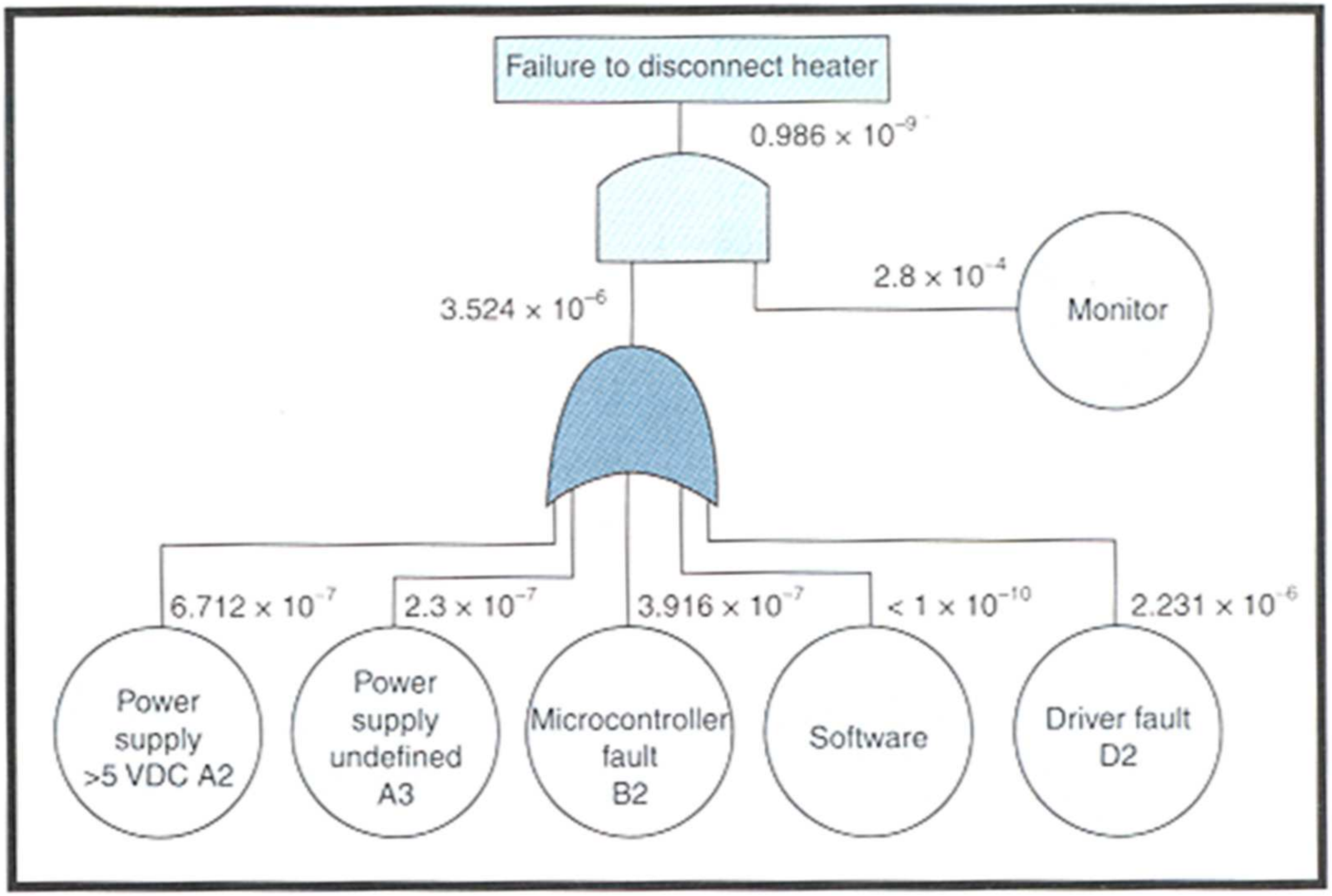
Monitor L1/Q1/Q2 current

check thermistor voltage

Allow micro to insert fault as a self-test

bad notation

Adding Hardware Monitor

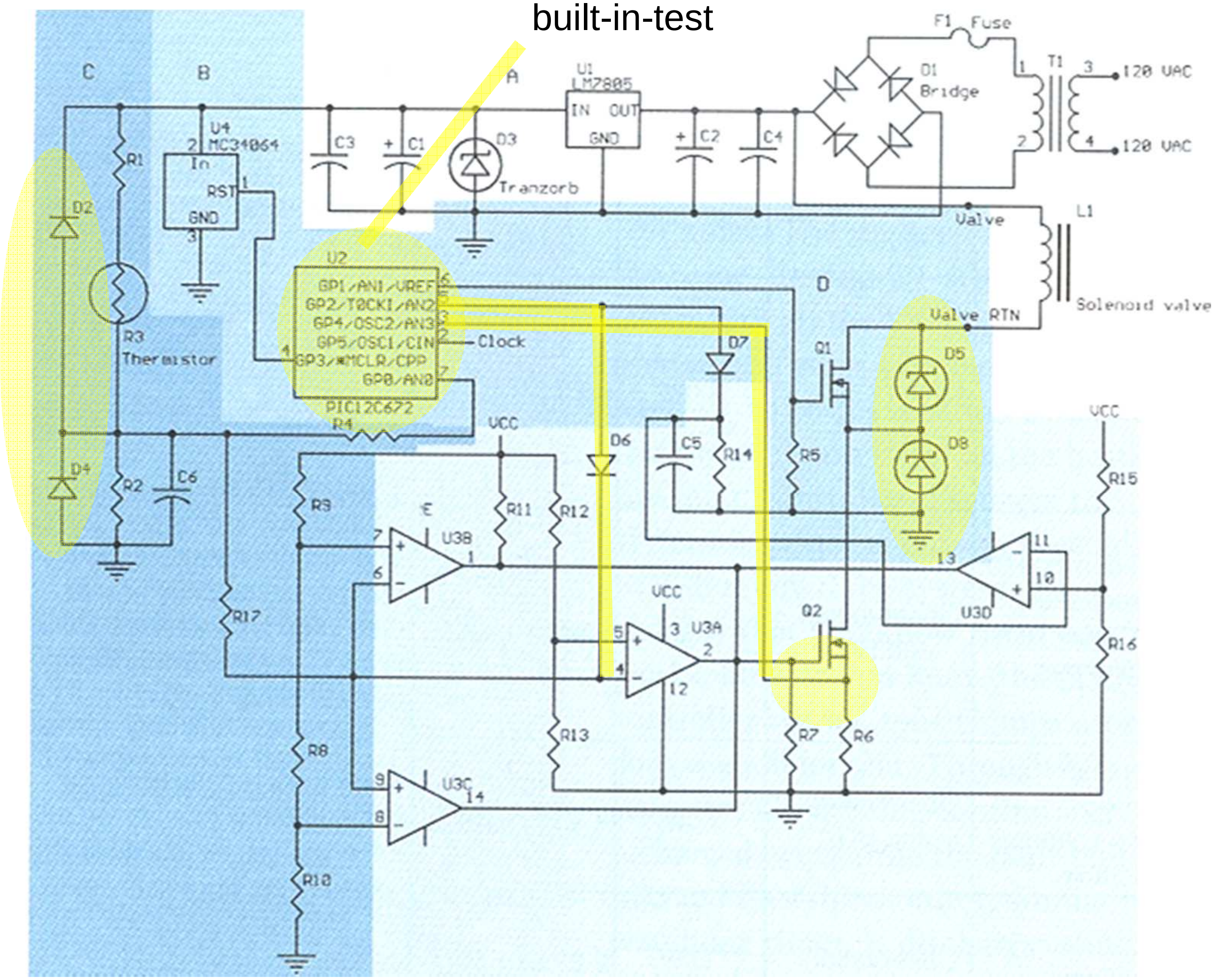


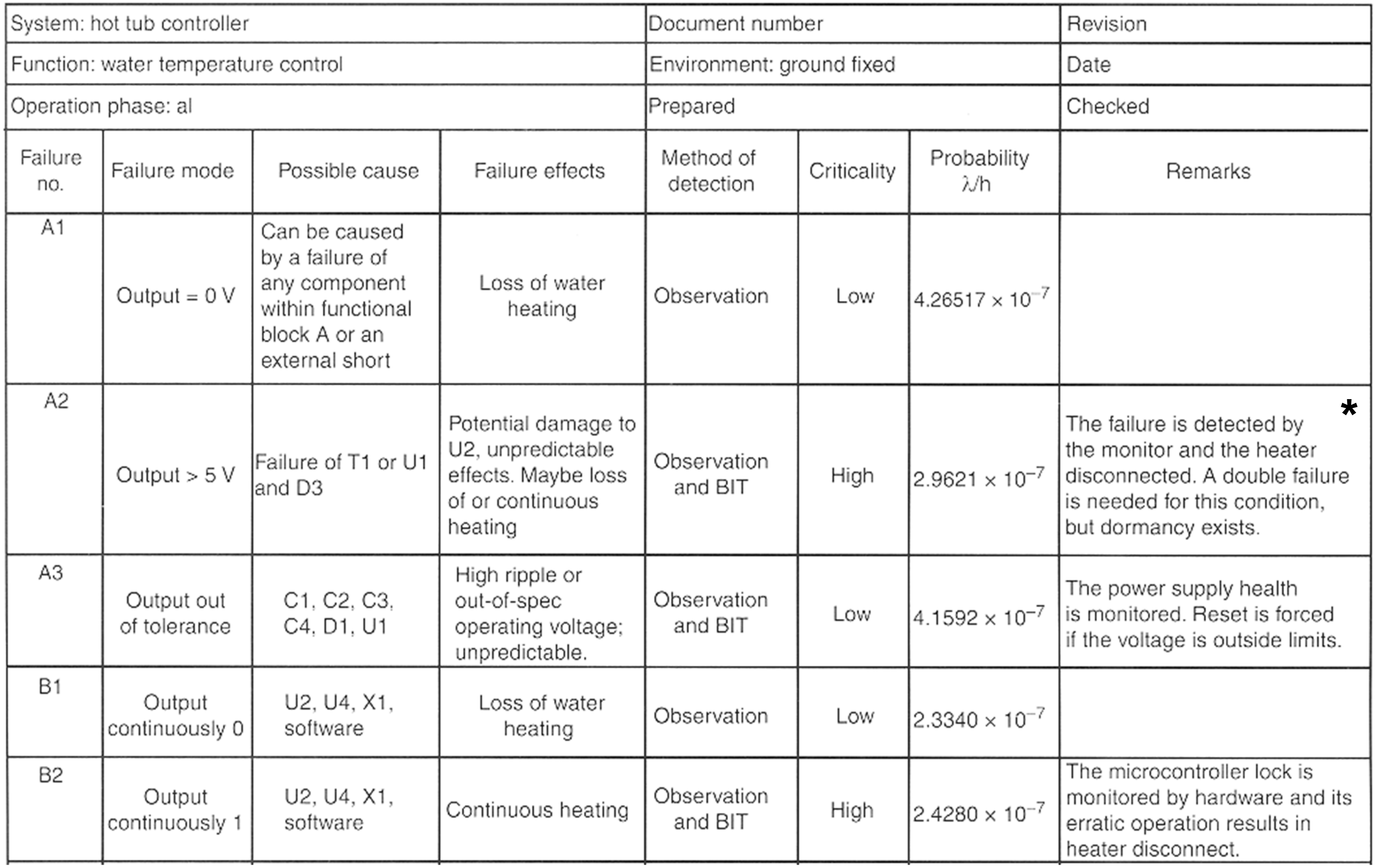
Added Redundancy

- **Microcontroller – performs sanity check on thermistor output**
  - **short/open would cause voltage to move out of plausible range**
  - **abrupt change in temperature would indicate fault**
- **Comparators (monitor circuit)**
  - **turn off Q2 if temperature exceeds upper limit**
  - **provide window for plausibility testing of temperature sensor**
- **Difficult part: eliminating dormant failures (all faults must be detected)**

Final Design

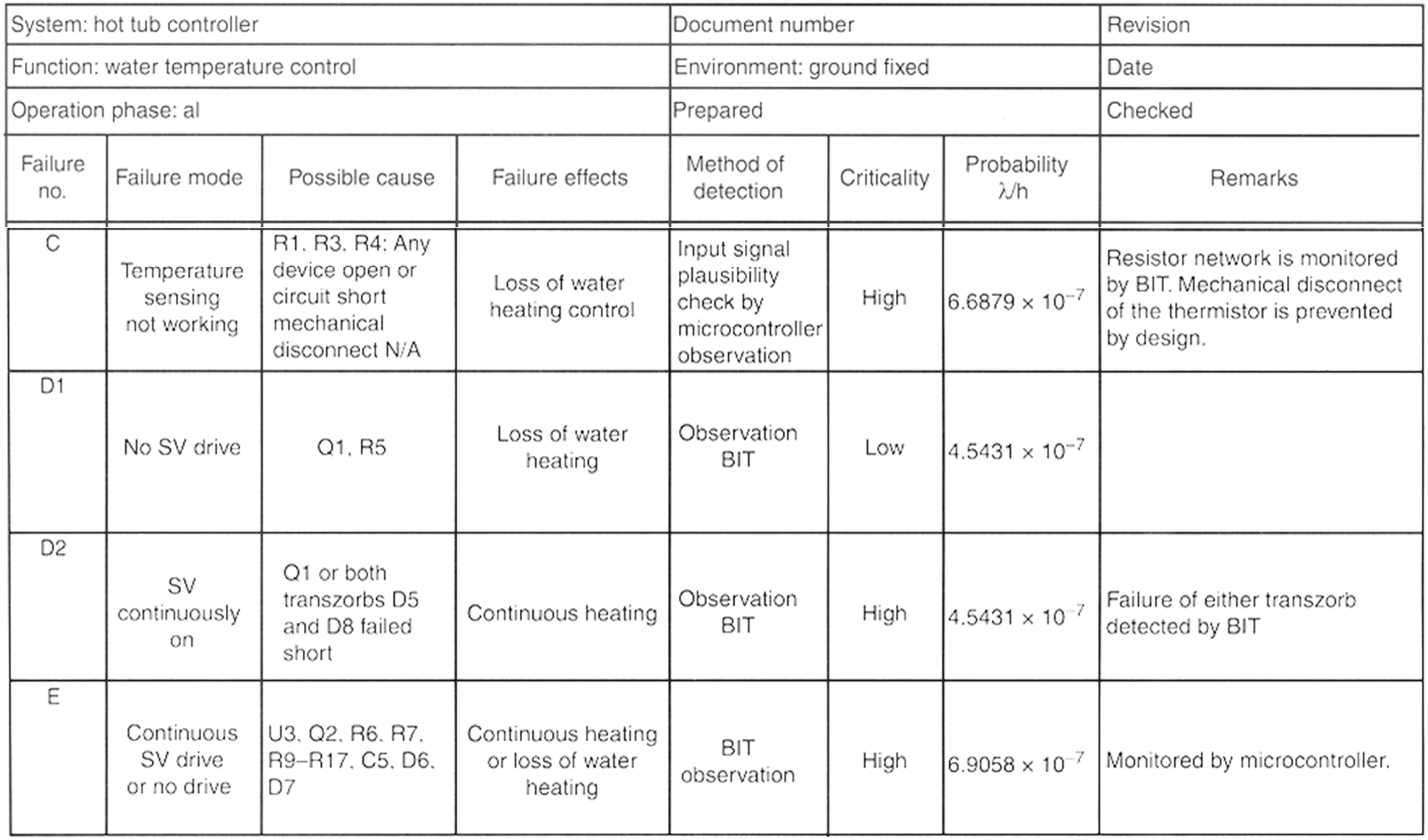
software monitors,
built-in-test





System: hot tub controller				Document number			Revision
Function: water temperature control				Environment: ground fixed			Date
Operation phase: al				Prepared			Checked
Failure no.	Failure mode	Possible cause	Failure effects	Method of detection	Criticality	Probability λ/h	Remarks
A1	Output = 0 V	Can be caused by a failure of any component within functional block A or an external short	Loss of water heating	Observation	Low	4.26517×10^{-7}	
A2	Output > 5 V	Failure of T1 or U1 and D3	Potential damage to U2, unpredictable effects. Maybe loss of or continuous heating	Observation and BIT	High	2.9621×10^{-7}	* The failure is detected by the monitor and the heater disconnected. A double failure is needed for this condition, but dormancy exists.
A3	Output out of tolerance	C1, C2, C3, C4, D1, U1	High ripple or out-of-spec operating voltage; unpredictable.	Observation and BIT	Low	4.1592×10^{-7}	The power supply health is monitored. Reset is forced if the voltage is outside limits.
B1	Output continuously 0	U2, U4, X1, software	Loss of water heating	Observation	Low	2.3340×10^{-7}	
B2	Output continuously 1	U2, U4, X1, software	Continuous heating	Observation and BIT	High	2.4280×10^{-7}	The microcontroller lock is monitored by hardware and its erratic operation results in heater disconnect.

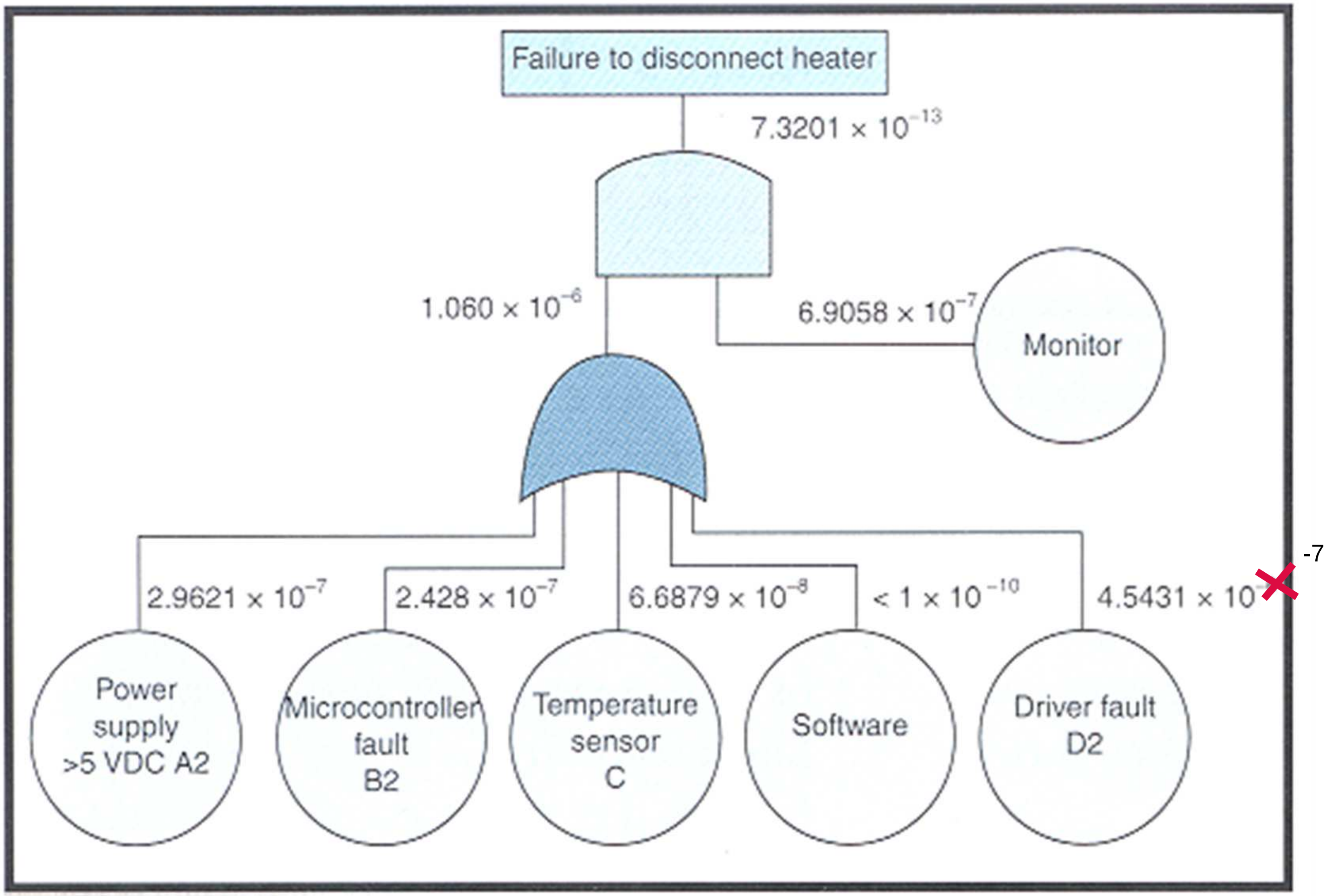
* assumes the analog circuitry can tolerate higher voltages



System: hot tub controller				Document number			Revision
Function: water temperature control				Environment: ground fixed			Date
Operation phase: al				Prepared			Checked
Failure no.	Failure mode	Possible cause	Failure effects	Method of detection	Criticality	Probability λ/h	Remarks
C	Temperature sensing not working	R1, R3, R4: Any device open or circuit short mechanical disconnect N/A	Loss of water heating control	Input signal plausibility check by microcontroller observation	High	6.6879×10^{-7}	Resistor network is monitored by BIT. Mechanical disconnect of the thermistor is prevented by design.
D1	No SV drive	Q1, R5	Loss of water heating	Observation BIT	Low	4.5431×10^{-7}	
D2	SV continuously on	Q1 or both transzorbs D5 and D8 failed short	Continuous heating	Observation BIT	High	4.5431×10^{-7}	Failure of either transzorb detected by BIT
E	Continuous SV drive or no drive	U3, Q2, R6, R7, R9–R17, C5, D6, D7	Continuous heating or loss of water heating	BIT observation	High	6.9058×10^{-7}	Monitored by microcontroller.

IMPORTANT RESULT: All high criticality failures are monitored

Final Design



Software and Watchdogs

- **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)**

Maintainability

- **Reliability predication indicates that after 10,000 units shipped, will need to service two problems per day**
- **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 & Compliance

Many categories in consumer electronics:

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.

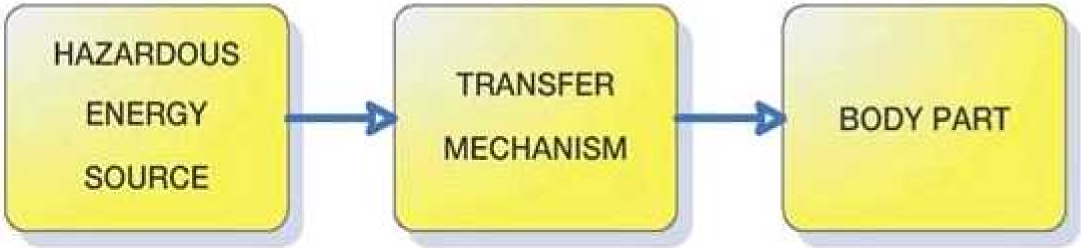
Example of a category relevant to ECE 477

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

From electronicdesign.com

The ABCs of IEC 62368-1, An Emerging Safety Standard

Date 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 the energy transfer to the body part.