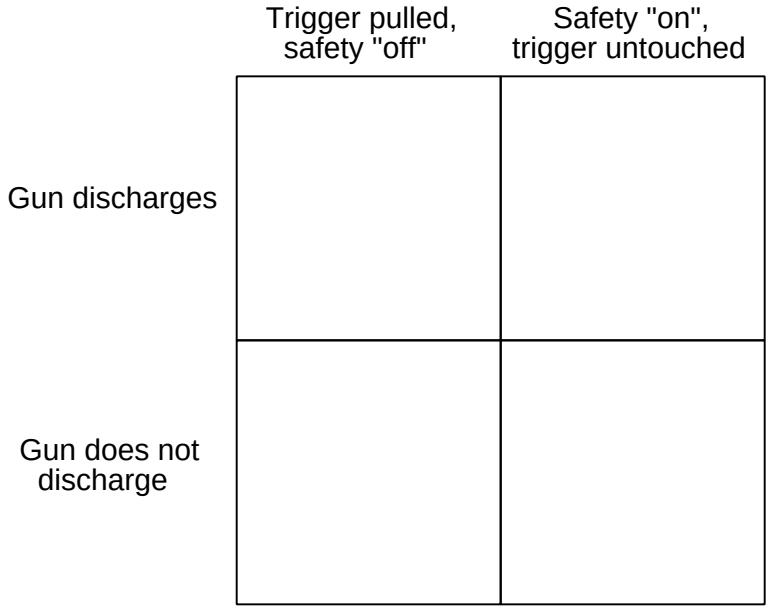
Probability calculations

Question 1

Apply the concepts of *dependability*, *security*, *PFD*, and *RSA* to the context of a firearm. Label each quadrant of the following chart with these terms (note: some of them may be synonymous, and not all quadrants may have an appropriate term in this list!):



Which of these quadrants represents desirable conditions, and which represent undesirable conditions? Are there any laws of probability applicable to the quadrants, assuming we had probability values associated with each?

Suggestions for Socratic discussion

- Label each of the quadrants with the Boolean terms D, S, $\overline{D}$, and $\overline{S}$ as appropriate.

file i03021

Question 2

Perform an experiment where you roll a set of dice to simulate a test of component reliability. Each die represents a single component being tested, with a random chance of failure following each roll. This experiment works better the more dice you have to roll (10 dice is a good minimum).

The purpose of this experiment is to contrast the scenarios of no component replacement versus immediate repair of any failed components, and also to gain a more intuitive understanding of MTBF (or MTTF). Count any die landing on "1" as a failed component, and landing on any other number as a surviving component.

First, perform successive rolls, removing any failed components after each roll so that the group of failed components grows over time while the group of surviving components (the only dice being rolled the next throw) dwindles over time. Record the sizes of the "failed" and "surviving" groups after each roll. For example:

Roll	**Total number failed**	**Number surviving**
0	0	15
1	2	13
2	3	12
3	5	10

Plot the results on a graph, noting the number of rolls required until 63.2% of the original components had failed.

Next, perform successive rolls, "repairing" any failed components after each roll so that each roll begins with the same number of total components. Record an accumulating total of "failures" after each roll. For example:

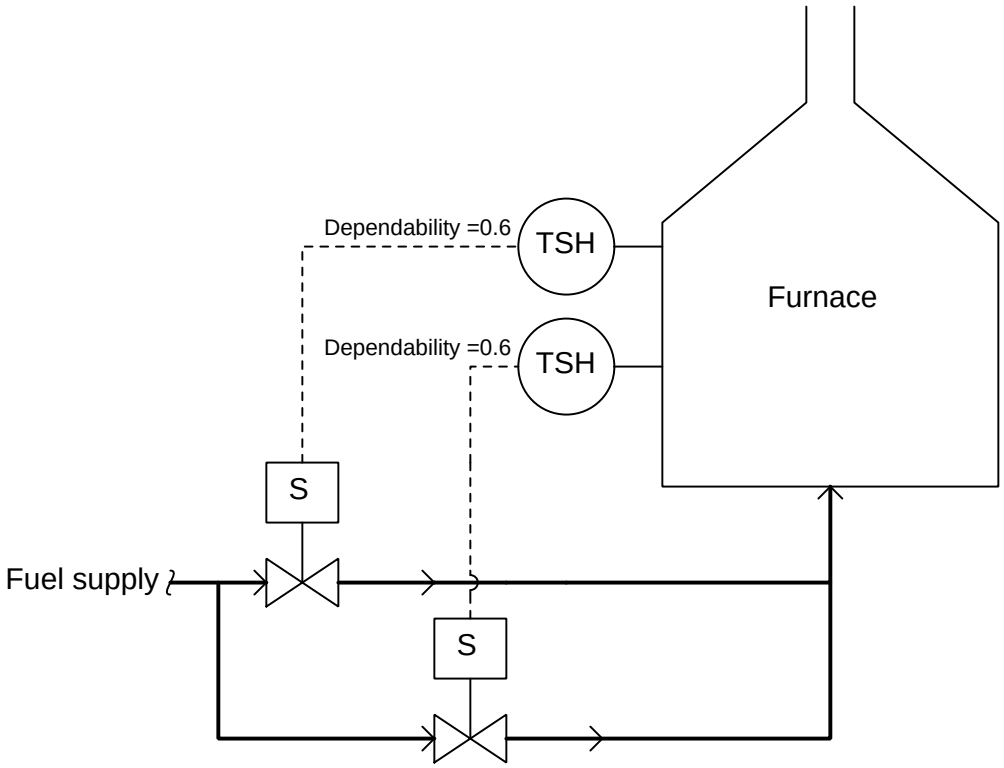
Roll	**Total number failed**	**Number surviving**
0	0	15
1	2	15
2	4	15
3	7	15

Plot the results on a graph, noting the number of rolls required until the accumulated number of failed components equals the total number of components maintained.

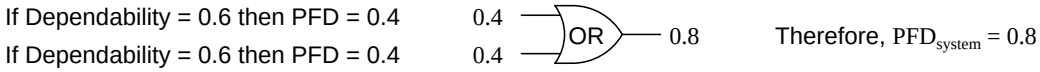
file i02497

Question 3

In this high-temperature safety shutdown system, fuel shuts off to the burner only if *both* high-temperature switches and shutoff valves properly function. Both switches have the same trip point, and both solenoid valves work identically. The dependability rating for each switch/valve set is 0.6, which means each one is known to properly shut off fuel flow in the event of a high-temperature condition 60% of the time:



A technician decides to calculate the probability of this system failing on demand. That is, he intends to calculate how likely it will be that gas could continue to flow to the furnace even when the temperature was too high. This is the technician's work to solve the problem:



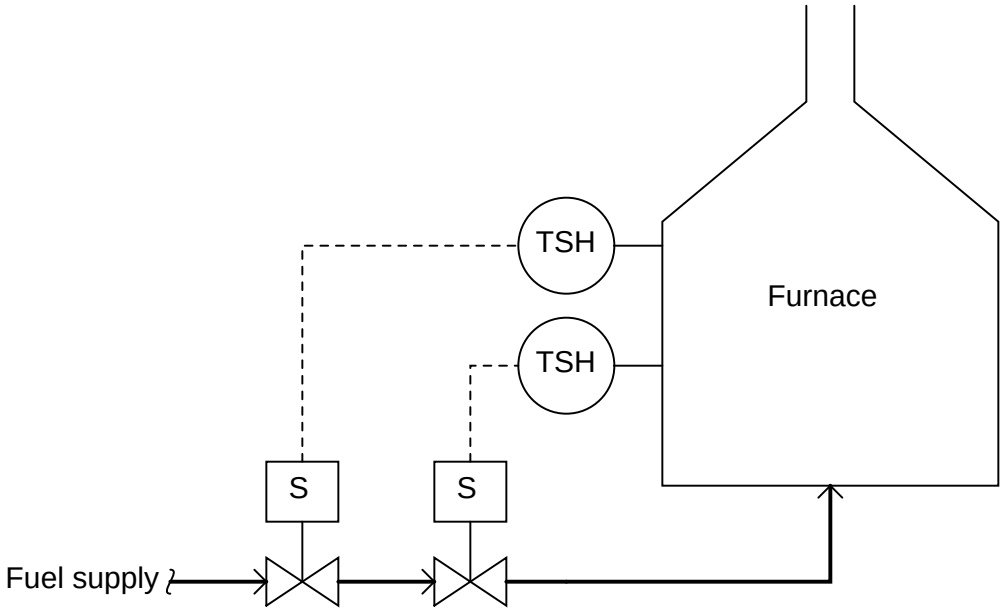
Identify both what is correct and what is incorrect in this technician's analysis of the system.

file i03599

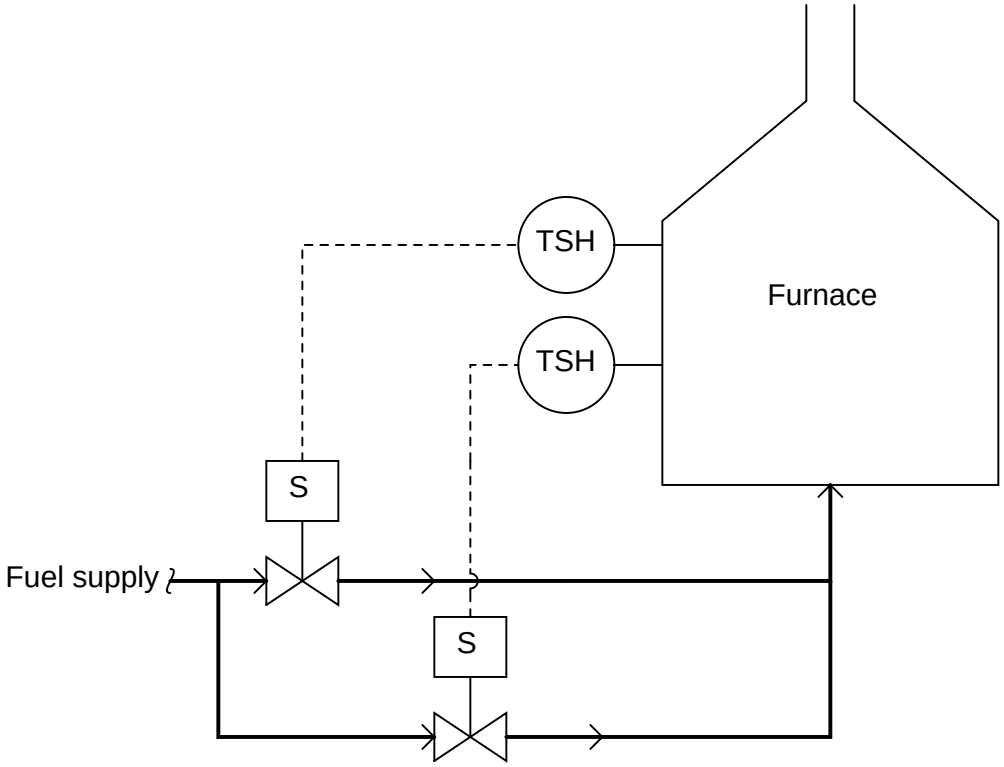
Question 4

All devices fail – it is not a question of "if," but "when." Given this fact, it is logical to provide dangerous processes with *redundant* control components, so that system safety is never dependent on any single component.

For example, suppose we wished to equip a furnace with a high-temperature safety shutdown system, to shut off fuel to the burner if ever the furnace temperature reached some critical value. Here, two high-temperature switches control two fuel shutoff valves. Both switches have the same trip point, and both solenoid valves work identically:



Here is another high-temperature shutdown system using redundant sensors and redundant safety valves. However, this system will not function the same as the previous system:



Determine which of these two redundant shutdown systems provides the greatest level of *dependability* (i.e. preventing over-temperature of the furnace), and which of them provides the greatest level of *security* (i.e. the ability to continue running the furnace when there is no overtemperature condition).

file i02487

Question 5

A team of instrument technicians is salvaging differential pressure transmitters from an abandoned process unit at an old facility. Upon removal, each transmitter is tested for proper operation. At the end of this salvage operation, 53 transmitters were found to be good and 8 were found to be defective.

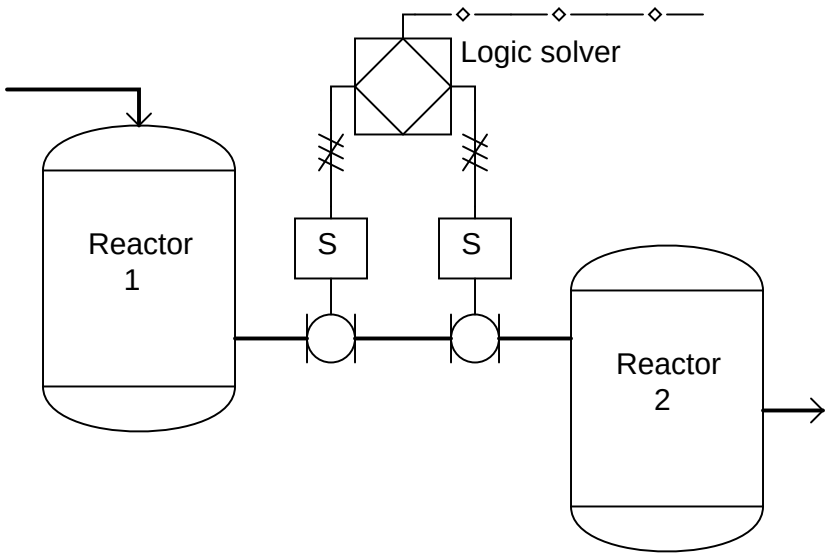
Unfortunately, all 61 transmitters were placed in the same crate, with no markings to designate which were good and which were defective. Suppose you were to randomly grab a transmitter from this crate: what is the probability that the transmitter will be good? Now, supposing the first transmitter you found was good; what is the probability that the *next* one you grab will be good?

Finally, calculate the probability that the *first two* transmitters you grab from this bin will both be good.

file i02498

Question 6

Two emergency isolation valves are installed in a process line between two chemical reactor vessels:



These safety shutdown valves normally spend their time in the wide-open position. Only during emergencies are they expected to close shut. Two are placed in series so that even if one isolation valve fails to shut when needed there will be another available to do the job.

Suppose the probability of each isolation valve failing on demand (PFD) is equal to 1.5×10^{-4}, given the age of the valves and actuators, and the frequency of partial-stroke testing. (Note, the PFD value will be different for valves of different age, and for different testing intervals.)

Calculate the probability of failure on demand of the two isolation valves *together*: the chance that *neither* valve will shut when needed during an emergency. Next, calculate the probability that this isolation system will work properly when needed (i.e. the probability that at least one of the two isolation valves will function properly on demand).

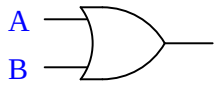
Suggestions for Socratic discussion

- Does placing two isolation valves in series prioritize *dependability* or does it prioritize *security*?
- Identify at least one important assumption implicit in the probability calculations shown here.

file i02502

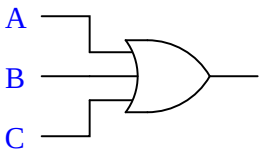
Question 7

The probability calculation for a logical two-input OR function follows this formula, where A and B are probability values ranging between 0 and 1 inclusive:



$$\text{Two-input OR function probability} = A + B - AB$$

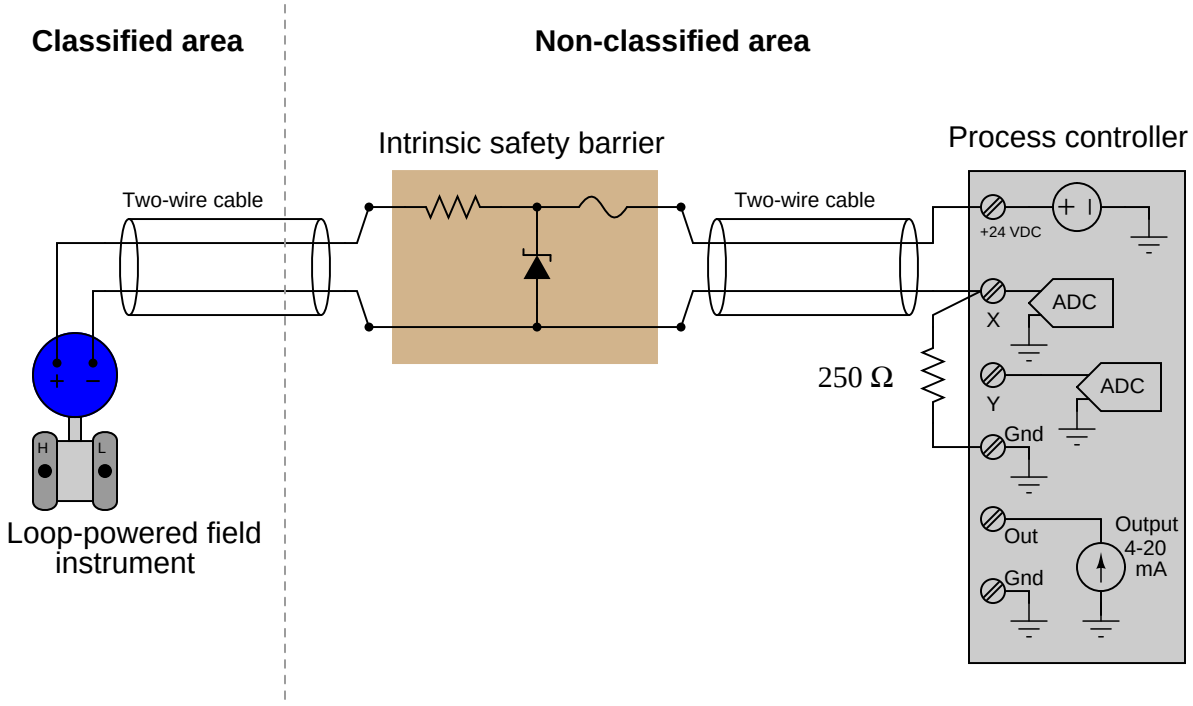
Derive a probability value formula for a *three-input* logical OR function:



file i01174

Question 8

An *intrinsic safety barrier* circuit is essential for making loop-powered 4-20 mA instrument systems "intrinsically safe." Explain what intrinsic safety means for an instrument system such as this, and also how the components inside the barrier circuit make the circuit intrinsically safe:



Supposing the resistor inside this intrinsic safety barrier has a probability of 2.4×10^{-6} of failing open, and the diode has a probability of 1.3×10^{-4} of failing shorted, calculate the probability that either of these two failures will interrupt the transmitter's signal from getting to the controller.

Supposing the fuse inside the barrier has a probability of 5.8×10^{-4} of failing open. How does this affect the probability of signal interruption for any barrier component failure?

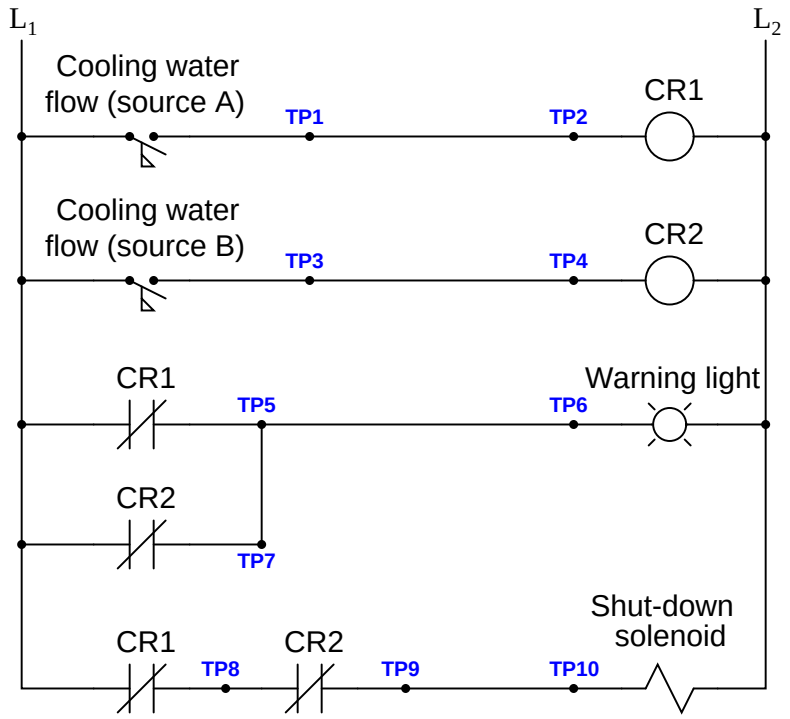
Suggestions for Socratic discussion

- A good reasoning technique to apply if you are having difficulty explaining the purpose of something is to explain the converse: what things would be like it that something were *not* present. In this case, explain why the circuit could be unsafe without the barrier in place, assuming certain circuit faults such as opens and shorts in the classified field location.
- Will the presence of an intrinsic safety barrier guarantee safe operation for *any* device installed in a classified area, or must the field devices themselves also be designed and rated for intrinsic safety?
- Would the loop-powered transmitter circuit still be considered intrinsically safe if the barrier were not present? Would it be considered non-incendive?
- Which of the two components inside the barrier poses the greatest risk to reliability, based on the failure probabilities?

file i02471

Question 9

A water-cooled generator at a power plant has two sources of cooling water flow, each source equipped with a flow switch that returns to its normal status (open) if the water flow through the pipe drops to too low of a rate:



Classify the alarm and the shutdown functions, each using *MooN* notation.

Given the following component dependabilities (and neglecting all other dependabilities in the system such as the power source), calculate the dependability of the alarm function and also the dependability of the shutdown function:

- Dependability of each flow switch = 0.993
- Dependability of each control relay = 0.9991
- Dependability of lamp = 0.998
- Dependability of shutdown solenoid = 0.965

Supposing you were assigned the task of testing this alarm/shutdown system as thoroughly as possible without actually interrupting water flow through either of the cooling water pipes, or actually shutting the generator down, design a testing procedure to determine as much as possible the readiness of this alarm/shutdown system. Points to identify in your procedure:

- Any electrical connections you would need to temporarily break
- Any temporary "jumper" connections you would need to make
- What you would detect or measure as confirmation that the system works as designed
- The order in which all steps would need to be done

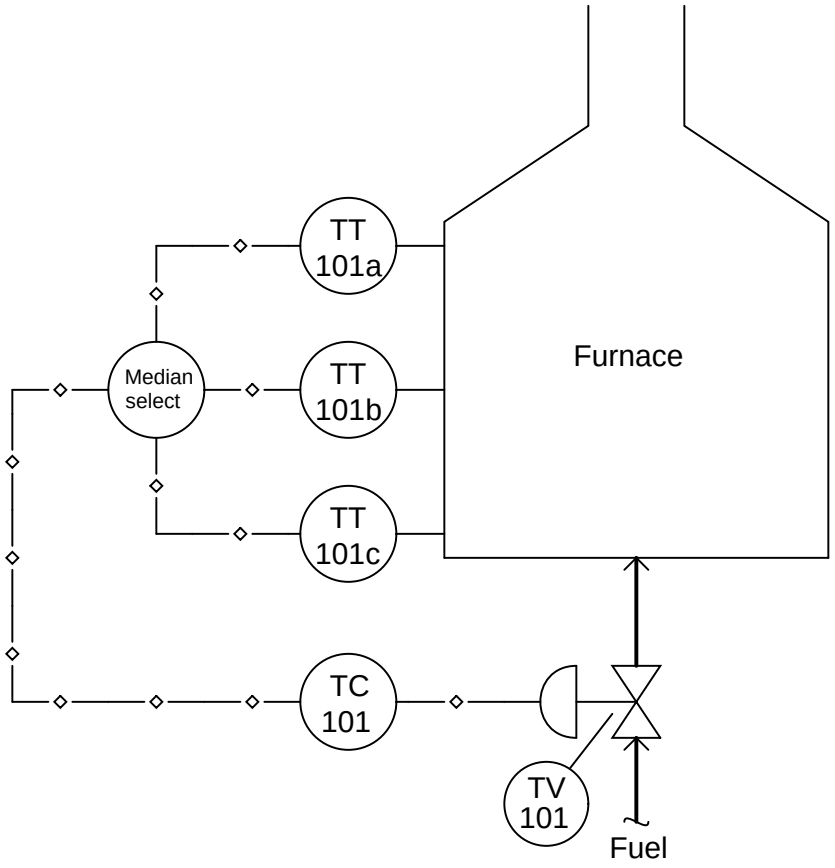
Suggestions for Socratic discussion

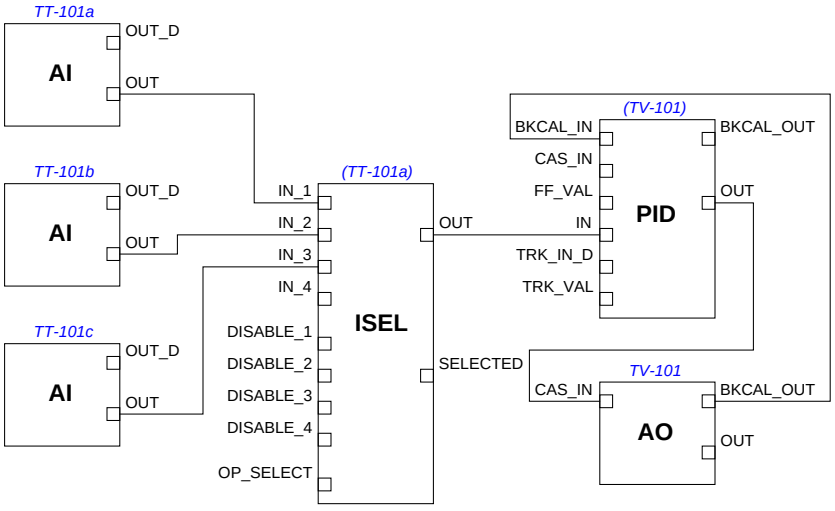
- Identify any safety precautions to follow when working on a "live" 120 VAC circuit (e.g. the *one-hand* rule).
- Are the flow switches' *normal* state the same as their *typical* state when the system is running as it should? Explain the distinction between "normal" and "typical" in this context.

file i03198

Question 10

A triple-redundant temperature control system is implemented using FOUNDATION Fieldbus technology. A general P&ID of the control scheme is shown here, followed by the Fieldbus function block diagram:





The ISEL function block selects the median signal from the three temperature transmitters, and is able to operate even if only one of those temperature signals is good.

Calculate the probability of system failure given the following device failure probabilites:

- TT-101a = 0.001
- TT-101b = 0.001
- TT-101c = 0.001
- TV-101 = 0.003

Now, suppose the ISEL function block were moved from TT-101a to TV-101. Re-calculate the probability of system failure given the same device failure probabilities.

file i02133

Question 11

Suppose a safety valve (a "chopper" valve) used to shut off flow during emergency conditions has a probability of failing to shut off when commanded to shut of 0.00014, and a probability of shutting off needlessly when commanded to stay open of 0.00033. Determine the following quantities in relation to this valve:

- Dependability (D) = _____
- Undependability ($\overline{D}$)= _____
- Security (S) = _____
- Unsecurity ($\overline{S}$) = _____

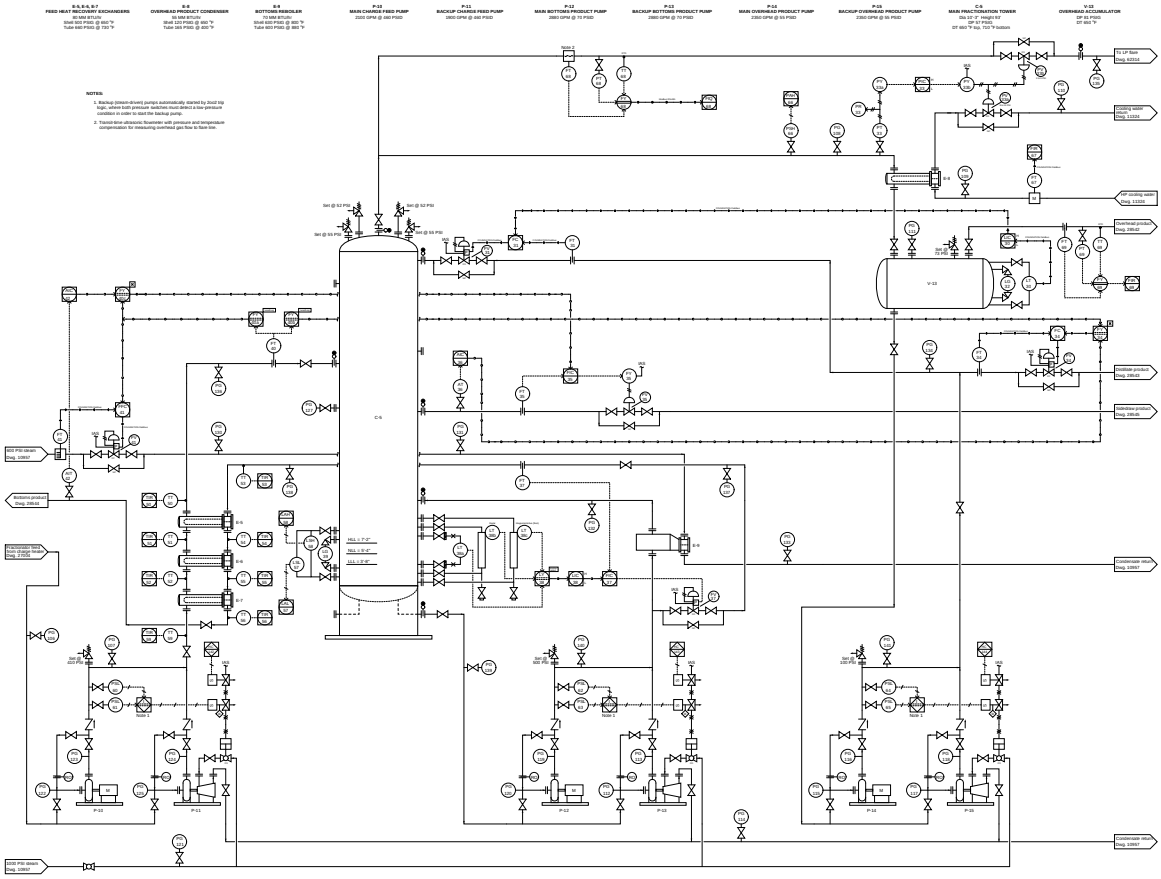
Next, calculate the RSA and PFD values for this valve.

Finally, calculate the *reliability* of this valve: the probability that it will act as commanded under all conditions.

file i02559

Question 12

Each of the electric-driven pumps in this distillation process is backed up by a redundant steam-driven pump, automatically started by a system using redundant pressure switches to sense low discharge pressure from the electric pump:



Suppose PSL-62 has a PFD value of 0.0051 and PSL-63 has a PFD value of 0.0048. Calculate the *dependability* of these two redundant pressure switches (i.e. the probability that together they will provide the necessary signal(s) to the auto-start system of pump P-13 if the discharge pressure falls below their trip points).

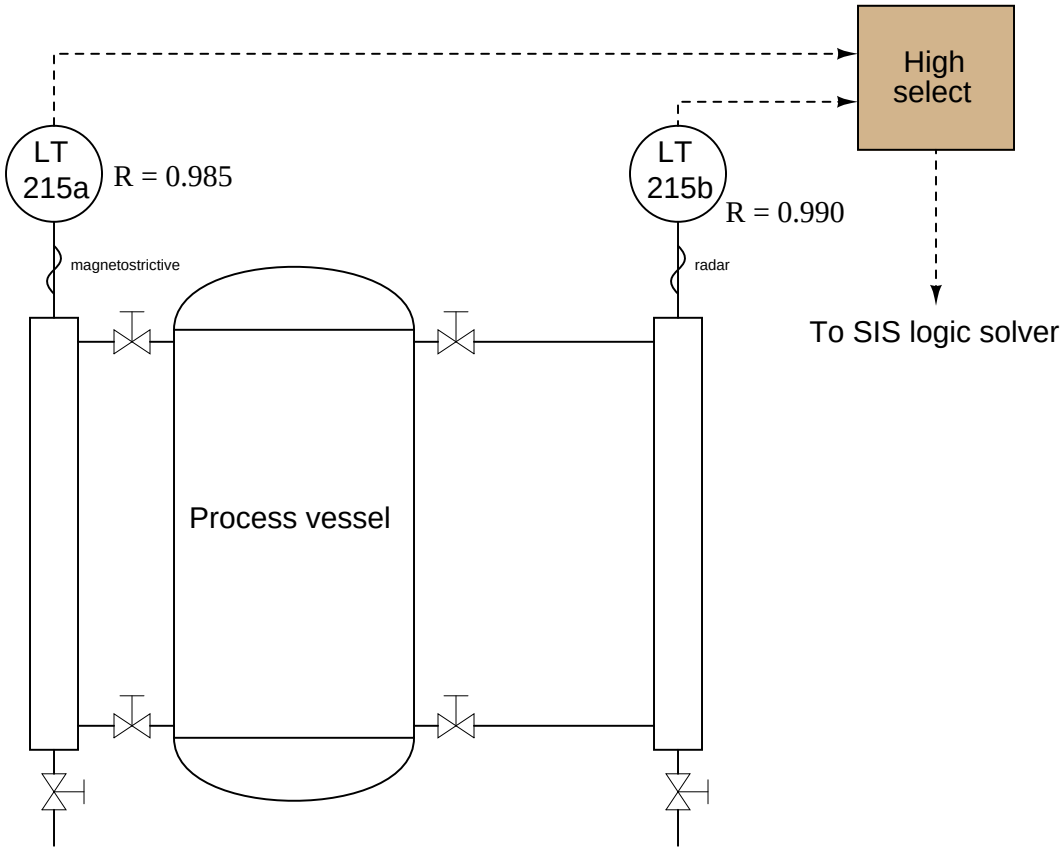
Suggestions for Socratic discussion

- A very helpful problem-solving technique when working with probabilities is to *sketch a logic function diagram* with each line in that diagram labeled with an easy-to-understand description of its real-life meaning. Sketch such a diagram for this problem, and then explain how that diagram is helpful.
- What other component or susbsystem PFD values would need to be considered in order to calculate the reliability of the entire auto-start system for pump P-13?
- What are the pressure relief valves at the top of the main fractionation tower set to different "lift" pressures?

file i02036

Question 13

Two different level transmitters are used as redundant sensing devices for a critical vessel in a petrochemical refining process where a high level condition is dangerous but a low level condition is safe. A "high select" voting algorithm ignores the lowest-reading transmitter signal. The reliability rating (R) for each transmitter – describing its probability of faithfully sensing liquid level inside the vessel – is shown on the diagram:



Determine the *MooN* ratings for this redundant transmitter system, from the perspective of *dependability* (i.e. the *MooN* rating describing its ability to detect a dangerous (high) level condition), as well as from the perspective of *security* (i.e. the *MooN* rating describing its ability to keep the process running).

MooN (dependability) = _____ MooN (security) = _____

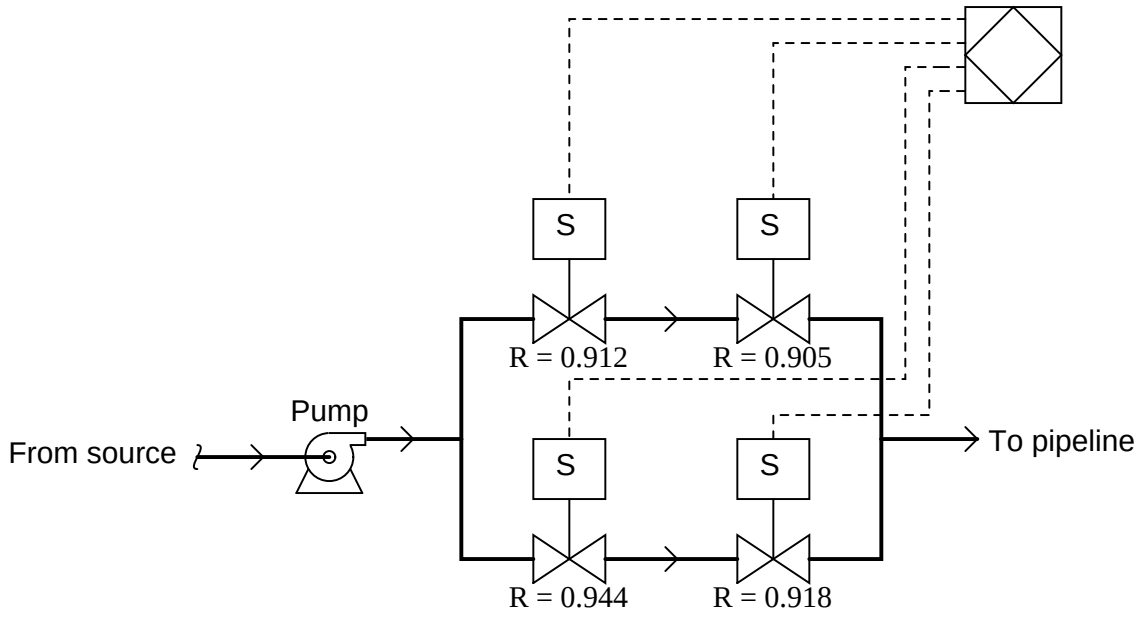
Next, calculate the overall reliability that this two-transmitter system will be able to initiate a shutdown if needed, based on the individual reliability ratings given:

$R_{shutoff}$ = _____

file i00225

Question 14

Four solenoid-actuated block valves are used as safety shutoff devices for a petroleum pipeline, all of them signaled simultaneously by one "logic solver" controller. The reliability rating (R) for each block valve – describing its probability of faithfully obeying the signal from the logic solver – is shown on the diagram:



Determine the *MooN* ratings for this four-valve block system, from the perspective of *dependability* (i.e. the *MooN* rating describing its ability to guarantee a shut-off pipeline), as well as from the perspective of *security* (i.e. the *MooN* rating describing its ability to guarantee a flowing pipeline).

MooN (dependability) = _____ MooN (security) = _____

Next, calculate the overall reliability that this four-valve block system will be able to guarantee shut-off of the pipeline, based on the individual reliability ratings given:

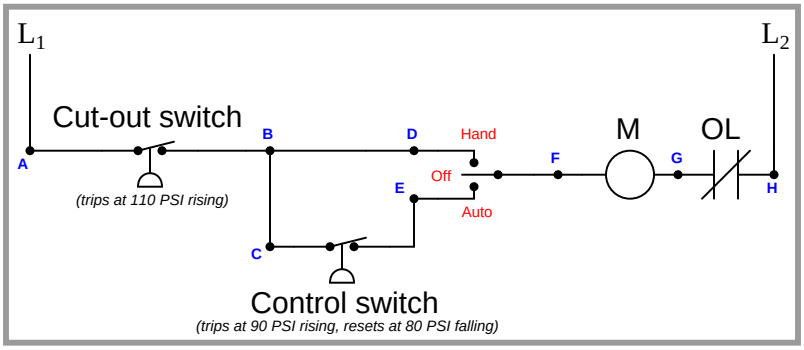
$R_{shutoff}$ = _____

file i00218

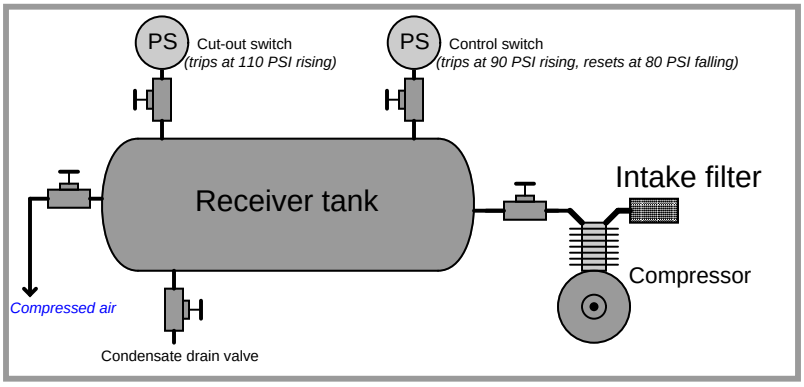
Question 15

The following circuit controls the starting and stopping of a motor-driven air compressor. The "M" coil is the coil of a three-phase contactor relay sending 480 VAC to the compressor's electric motor. The "OL" contact is a thermal overload contact (similar to a "51" time-overcurrent protective relay) which forces the contactor to de-energize and cut power to the motor if the motor draws too much current over time:

Control circuit schematic



Pictorial diagram of system



Suppose you were asked to test the high-pressure "cut-out" switch for proper operation without shutting the compressor down to perform the test. Explain how you could perform this test safely while the compressor was running.

Also, calculate the PFD for unchecked overpressure (substantially above 110 PSI) given the following pressure switch dependability values, assuming the hand switch is left in the "Auto" position:

- Dependability$_{control}$ = 0.947
- Dependability$_{cutout}$ = 0.981

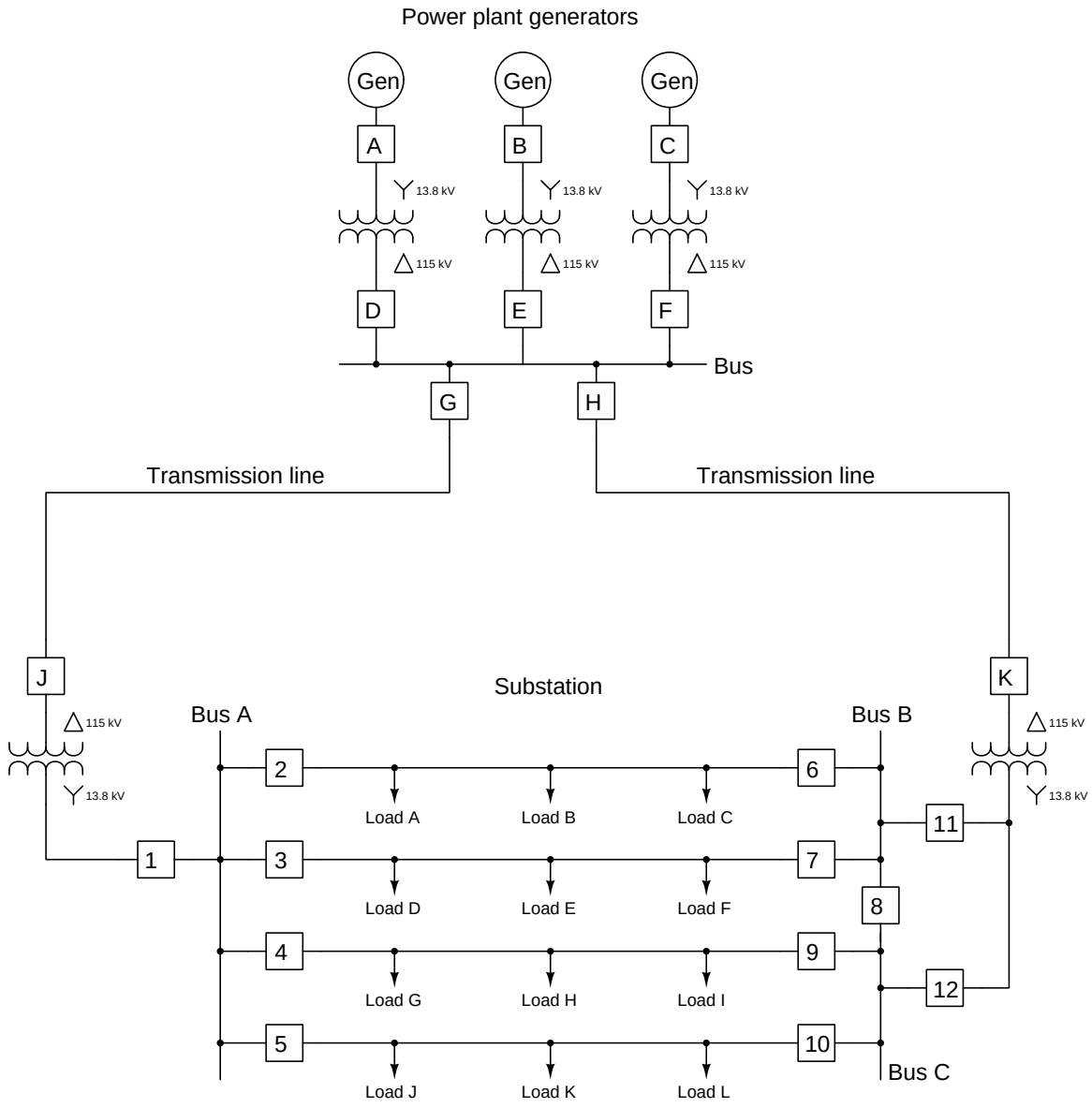
Suggestions for Socratic discussion

- Identify any safety precautions to follow when working on a "live" 120 VAC circuit (e.g. the *one-hand* rule).
- How would the PFD of this system be affected if the hand switch were left in the "Hand" position?

file i02110

Question 16

A very common form of schematic used to represent large-scale electric power systems is the *single-line diagram*, where all three phase conductors in a circuit are represented by single lines in the diagram. A single-line diagram showing a power plant sending power to a substation for distribution to business and residential loads is shown here:



A concern in electric power grids is *breaker failure*: when a circuit breaker fails to open as it should when given a "trip" signal. Suppose breaker #5 fails to open all its contacts when manually tripped.

Identify which other substation breakers must be tripped in order to isolate the failed breaker #5 from all power, after the breaker failure has been detected by a "breaker failure" relay monitoring breaker #5. How many loads (power customers) are affected by this subsequent action?

Suppose the PFD for each of breaker #5's three power contacts is 0.000273. Calculate the probability of *any* of these contacts failing to open when the breaker mechanism is tripped.

Also, how do you think a breaker failure might be detected by electronic devices? What diagnostic data would a breaker-failure detection circuit "look for" in order to determine a breaker had indeed failed to open all its contacts when tripped? Examine this photograph of a 125 kV SF_6 gas circuit breaker for clues:

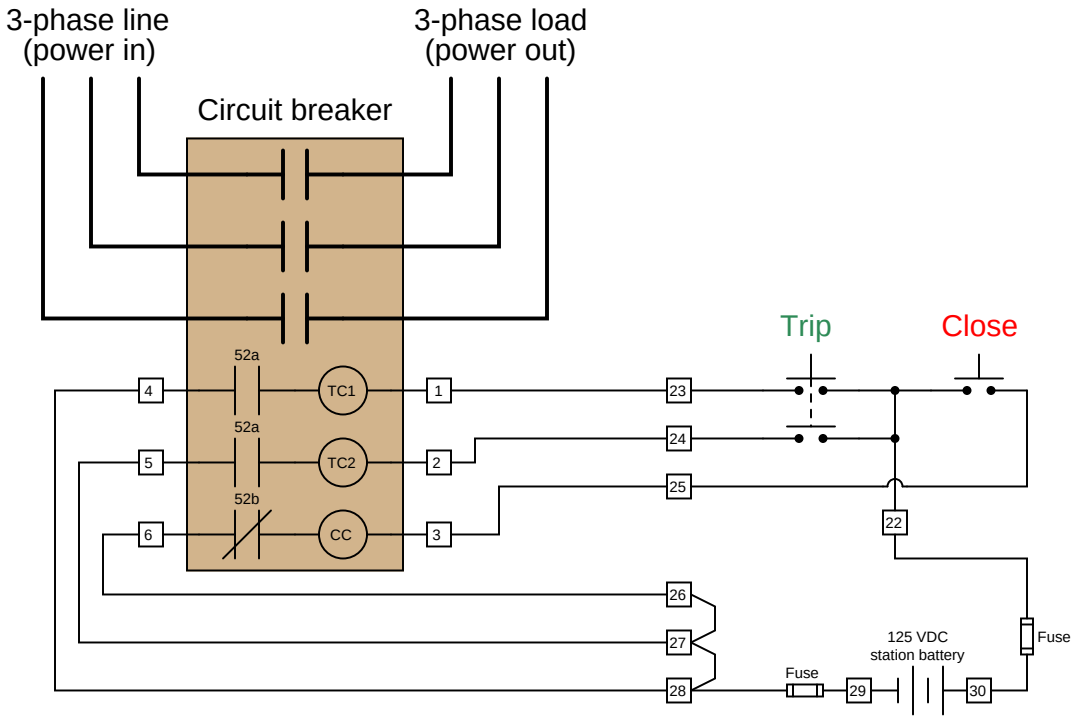
Suggestions for Socratic discussion

- Why do you suppose single-line diagrams are popular within the electrical power industry, rather than full schematic diagrams showing all power conductors?
- What would happen in this power system if breaker "F" were to trip?
- Suppose the dependability of each breaker in this system (i.e. the probability it will trip when called to trip) is 0.99918, and the security of each breaker in this system (i.e. the probability it won't trip when it's not supposed to) is 0.99993. Based on these figures, calculate the following probabilities:
  - → The probability that the right-hand transmission line cannot be isolated in the event of a fault.
  - → The probability that the left-hand transmission line will be unnecessarily removed from service (i.e. opened so it no longer carries load current).
  - → The probability that one particular generator will be taken off-line unnecessarily.
  - → The probability that *any* of the generators will be taken off-line unnecessarily.
  - → The probability that the high-voltage bus cannot be isolated in the event of a fault.
  - → The probability that the left-hand substation bus cannot be isolated in the event of a fault.
  - → The probability that the left-hand substation bus will become unnecessarily isolated.
  - → The probability that the entire substation will suffer an unnecessary outage.

file i02116

Question 17

A high-voltage circuit breaker is manually operated from a remote location using a pair of pushbutton switches, connected to "trip" and "close" solenoid coils within the breaker:



Note: the "52a" and "52b" contacts wired in series with the solenoid coils within the breaker are *auxiliary* contacts, actuated by the same mechanism as the three power contacts (i.e. 52a contacts are open when the power contacts are open, and closed when the power contacts are closed. 52b contact always exhibits the opposite state as the power contacts). The two trip coils are redundant: only one of them needs to energize in order to trip the circuit breaker.

Given the following dependability figures for each component, and assuming all other elements in the system are 100% reliable, calculate the probability of failure for breaker tripping (i.e. the probability that the breaker will *not* trip when the "Trip" pushbutton is pressed), and also the probability of failure for breaker closing (i.e. the probability that the breaker will *not* close when the "Close" pushbutton is pressed).

- Pushbutton contact = 0.991 (each)
- Coil = 0.99987 (each)
- Fuse = 0.9971 (each)
- Battery = 0.9984

PFD_{close} = _____

PFD_{trip} = _____

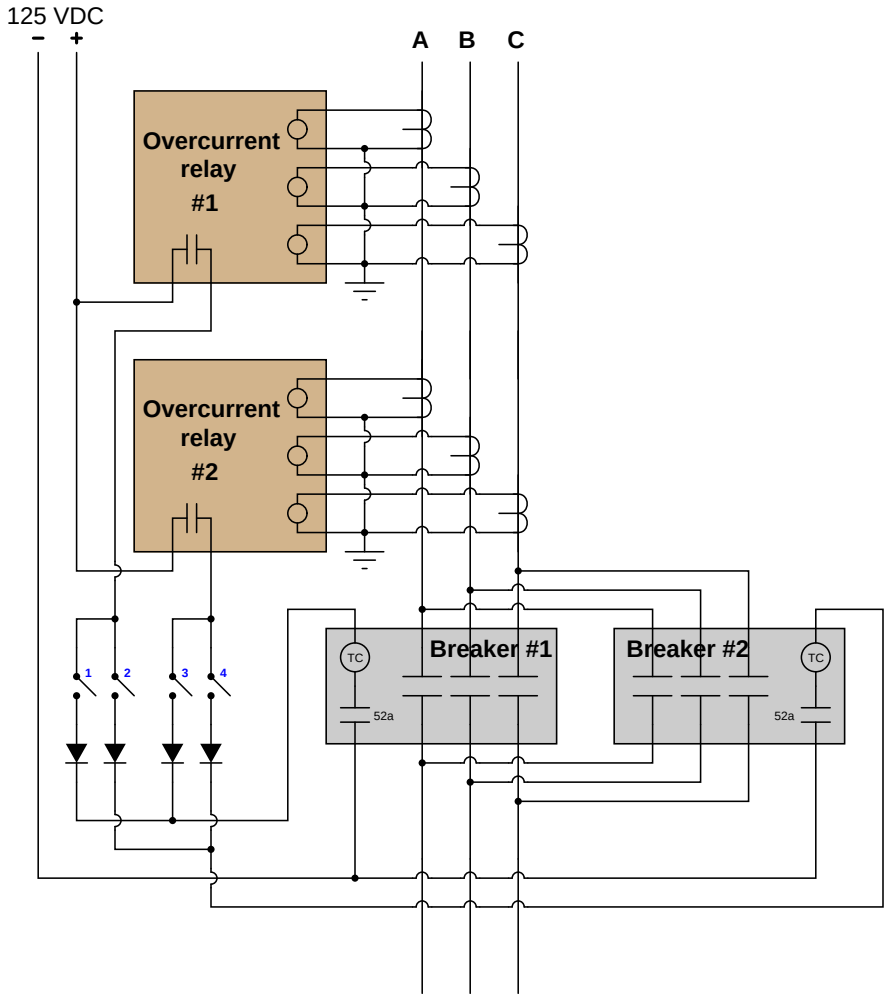
Suggestions for Socratic discussion

- Which function, tripping or closing, has the least probability of failure? Why do you think the system is designed this way?
- What is the purpose for having auxiliary contacts in the trip and close circuits?

file i01894

Question 18

Examine this schematic diagram for this protective relay system, where a pair of parallel circuit breakers are controlled by two redundant overcurrent relays:



Identify the switch closure positions necessary to have relay #1 control breaker #2, and have relay #2 control *both* breakers #1 and #2.

Explain why the diodes are in this circuit. Hint: these are sometimes referred to as *voting* diodes. They are not used for current-measurement (as in 4-20 mA circuits), nor do they suppress transient voltages (commutating diodes across inductive loads).

Given a dependability value of 0.99982 for each relay and a dependability value of 0.99961 for each circuit breaker, calculate the probability that the breakers will fail to trip in an overcurrent condition with all four relay/breaker selection switches in the closed position (assume all other system components are 100% reliable).

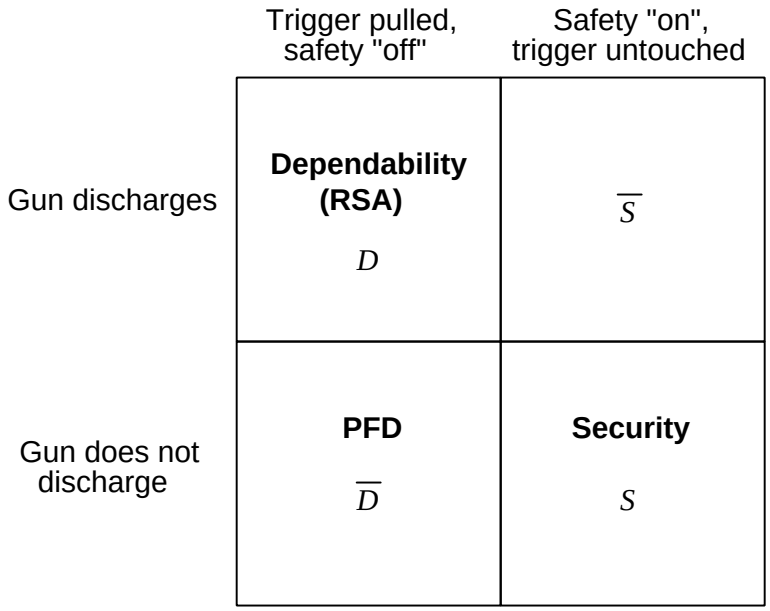
Suggestions for Socratic discussion

- A very useful problem-solving technique for figuring out the purpose of a particular device in a system is to analyze that system's behavior *without* the device in question. In this example, consider how the

system would function if the voting diodes were *not* installed in the trip circuitry.

file i02112

Answer 1



Probability values in the same column but in different rows (e.g. RSA versus PFD) are *mathematical complements* of each other, because their sum must be equal to 100% (1). For example, an RSA of 99.98% is equivalent to a PFD of 0.02% because there are only two (exclusive) possibilities of what will happen when the trigger is pulled and the safety is off: either the gun will fire or it will not fire.

Answer 2

Answer 3

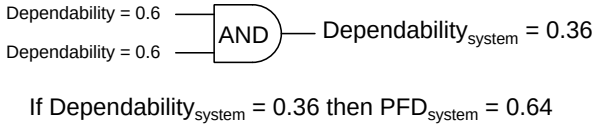
The technician was correct to apply the logical `OR` function here: the system will fail to protect against high temperature if either switch/valve set A *or* switch/valve set B fails. However, this is an *inclusive* `OR` function rather than exclusive, which means the proper equation to use is:

$$P = A + B - AB$$

$$P = 0.4 + 0.4 - (0.16)$$

$$P = 0.64$$

Another way to solve this is to calculate based on *dependability* rather than PFD. We can say that the system requires both switch/valve set A *and* switch/valve set B to function properly in order for the shutdown system to shut the furnace down. Thus:



If Dependability$_{system}$ = 0.36 then PFD$_{system}$ = 0.64

Answer 4

The first (series valves) system provides 1oo2 dependability and 2oo2 security. The second (parallel valves) system provides 2oo2 dependability and 1oo2 security.

Answer 5

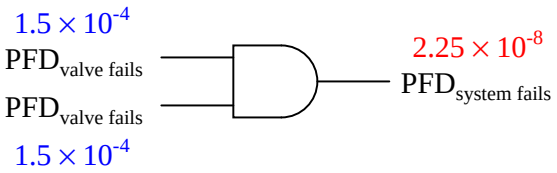
$P(\text{1st good}) = \frac{53}{61} = 0.86885$

$P(\text{2nd good}|\text{1st good}) = \frac{52}{60} = 0.86667$

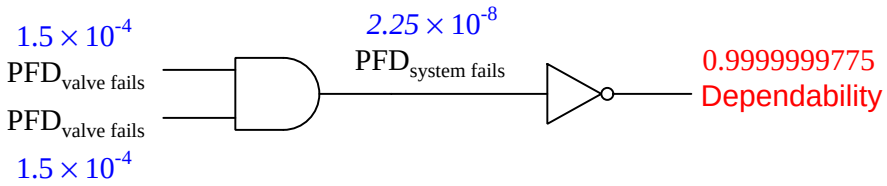
$P(\text{1st } \textit{and} \text{ 2nd good}) = \left(\frac{53}{61}\right)\left(\frac{52}{60}\right) = 0.75301$

Answer 6

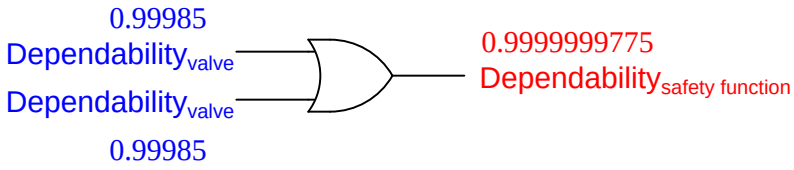
Since this is a series (double) block valve system, the probability that the safety function fails will be the probability that *both* block valves fail to shut on demand. Thus, the PFD for both valves together = 2.25×10^{-8}



The probability that this safety function will perform as designed and shut off the flow when needed (i.e. that is will be *dependable*) is the complement of its PFD:



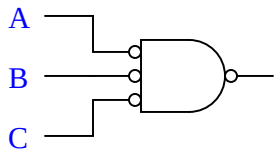
An alternative method for calculating the dependability of this system is to begin with the dependability figures for each block valve. If the PFD for each valve is 1.5×10^{-4}, then the dependability of each valve (i.e. the probability that it will shut off when it is supposed to) will be the complement of this value, or 0.99985. Since the dependability of the whole safety function is the probability that either or both of these block valves operates properly, we may model this as an OR function:



Note: if you are having trouble seeing the relationship between individual PFD's and the overall PFD of the system, try simplifying the problem. Consider each valve to be a 6-sided die, where rolling a "1" is equivalent to failing, and rolling anything else (2 through 6) is considered success. Now calculate the probability of failure for the whole system (i.e. both dice rolling "1").

Answer 7

We may use DeMorgan's Theorem to translate the three-input OR gate into a three-input AND gate with inverted inputs and outputs, then express the probability values accordingly:



$$\text{Three-input OR function probability} = 1 - [(1 - A)(1 - B)(1 - C)]$$

$$\text{Three-input OR function probability} = 1 - [(1 - B - A + AB)(1 - C)]$$

$$\text{Three-input OR function probability} = 1 - [1 - C - B + BC - A + AC + AB - ABC]$$

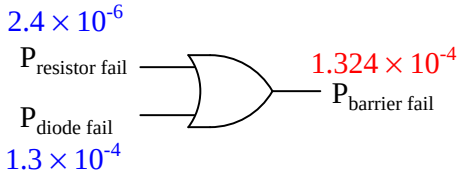
$$\text{Three-input OR function probability} = 1 - 1 + C + B - BC + A - AC - AB + ABC$$

$$\text{Three-input OR function probability} = A + B + C - AB - BC - AC + ABC$$

Answer 8

The intrinsic safety barrier protects against potential ignition resulting from short-circuits in the field wiring, and from over-voltage from the process controller power supply. I'll let you explain *how* the barrier circuit's components do this!

The probability of either the resistor or the diode interrupting the signal is a logical "OR" function, and so the calculation of probability takes this form:

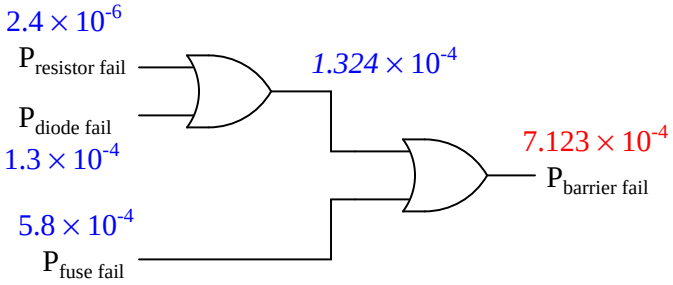


$$P(\text{A } or \text{ B}) = P(B) + P(A) - P(A) \times P(B)$$

$$P_{interruption} = (2.4 \times 10^{-6}) + (1.3 \times 10^{-4}) - [(2.4 \times 10^{-6})(1.3 \times 10^{-4})]$$

$$P_{interruption} = 1.324 \times 10^{-4}$$

Adding the fuse's fault probability into the mix is another "OR" function:



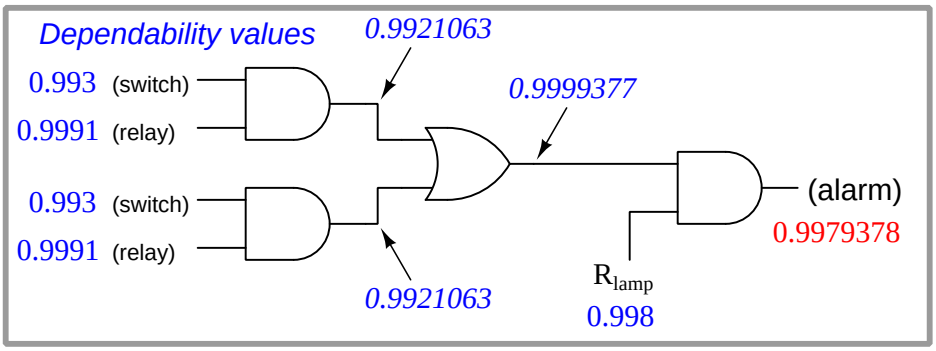
$$P_{interruption} = (1.324 \times 10^{-4}) + (5.8 \times 10^{-4}) - [(1.324 \times 10^{-4})(5.8 \times 10^{-4})]$$

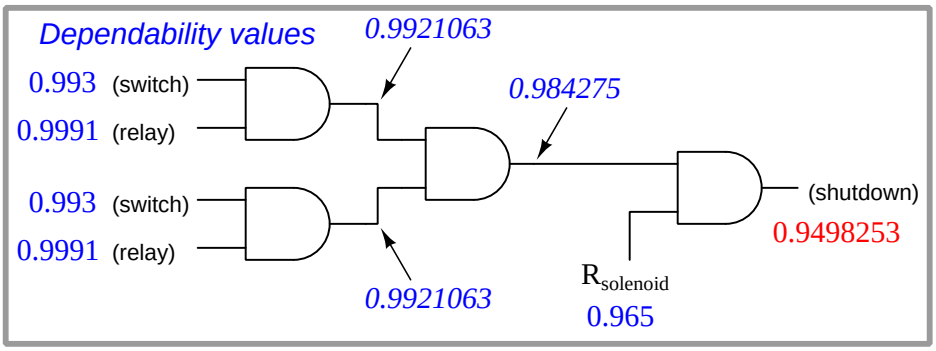
$$P_{interruption} = 7.123 \times 10^{-4}$$

Answer 9

This system provides 1oo2 alarm and 2oo2 shutdown functions.

Probability calculations using logic symbols:



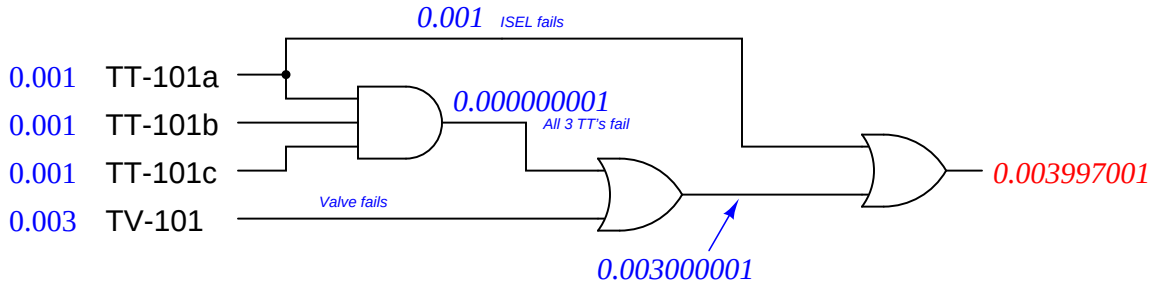


Trip test procedure (in order):

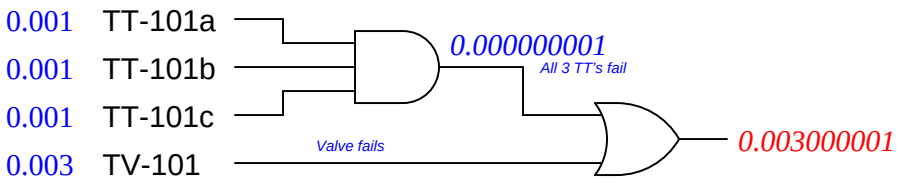
- Disconnect wire at TP9 or TP10 (disables shutdown solenoid)
- Connect voltmeter between TP9 and TP10
- Disconnect wire at either TP1 or TP2 – alarm light should come on
- Reconnect wire (TP1 or TP2) – alarm light should turn off
- Disconnect wire at either TP3 or TP4 – alarm light should come on
- Disconnect wire at either TP1 or TP2 – voltmeter should register supply voltage
- Reconnect wires (TP1 or TP2; TP3 or TP4)
- Remove voltmeter from circuit
- Reconnect wire at TP9 or TP10 (enables shutdown solenoid)

Answer 10

Probability of system failure with ISEL block located in TT-101a = 0.003997001



Probability of system failure with ISEL block located in TV-101 = 0.003000001



Answer 11

The given figures of 0.00014 and 0.00033 represent the valve's undependability and unsecurity, respectively. Dependability and security will be the mathematical complements of these values:

- Dependability $(D) = \underline{0.99986}$
- Undependability $(\overline{D}) = \underline{0.00014}$
- Security $(S) = \underline{0.99967}$
- Unsecurity $(\overline{S}) = \underline{0.00033}$

RSA (Required Safety Availability) is a synonym for dependability, and is equal to 0.99986. *PFD* (Probability of Failure on Demand) is a synonym for undependability, and is equal to 0.00014.

Reliability is the overall probability that the valve will do as commanded. This includes shutting off when commanded to shut (Dependability) and remaining open when not commanded to shut (Security). If we take all possible conditions of response to both command states and sum those probabilities together, we get a total of two (0.99986 + 0.00014 + 0.99967 + 0.00033 = 2). Since any probability is defined as the ratio of specific outcomes to total possible outcomes, in order to calculate reliability we must divide the probabilities of all correct actions (D + S) by the total value of all possible actions (2):

$$R = \frac{D+S}{2} = \frac{0.99986 + 0.99967}{2} = 0.999765$$

Answer 12

According to Note 1 in the P&ID, this is a 2oo2 trip system: *both* pressure switches must trip in order to start pump P-13. This means the dependability of the two switches taken together is less than the dependability of either switch on its own.

$\text{PFD}_{PSL-62} = 0.0051 \qquad R_{PSL-62} = 0.9949$

$\text{PFD}_{PSL-63} = 0.0048 \qquad R_{PSL-63} = 0.9952$

Since both switch PSL-62 *ans* PSL-63 must successfully trip on demand, the dependability for both in this 2oo2 system is an "AND" function (the mathematical product) of their individual dependabilities:

$(R_{PSL-62})(R_{PSL-63}) = (0.9949)(0.9952) = 0.99012448$

Answer 13

MooN (dependability) = **1oo2** MooN (security) = **2oo2**

$R_{shutoff}$ = **0.99985**

Answer 14

MooN (dependability) = **3oo4** MooN (security) = **3oo4**

$R_{shutoff}$ = **0.98709**

Answer 15

In order to test the high-pressure cutout switch, we could first jumper its terminals electrically so that the circuit will remain powered when the switch contacts open. Next, we can shut the block valve for that PSH and disconnect it from the circuit (as well as remove it from the vessel) and bring the switch back to the shop for testing.

Since this is a 1oo2 trip system, the probability that the system will reliably trip when needed is an OR function of the two switches' dependabilities (in other words, either one switch or the other needs to be dependable in order to avoid an overpressure condition):

$$P(\text{A } \textit{or } \text{B}) = P(B) + P(A) - P(A) \times P(B)$$

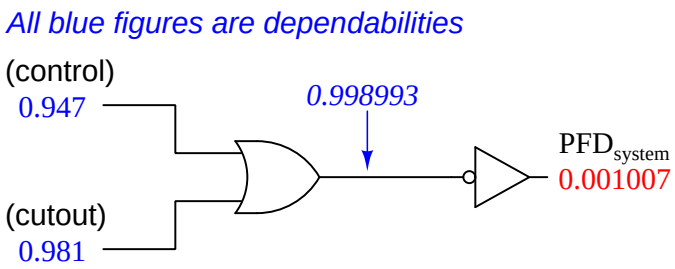
$$\text{Dependability}_{1oo2} = 0.947 + 0.981 - (0.947)(0.981)$$

$$\text{Dependability}_{1oo2} = 0.998993$$

Since we are looking for the probability that both these switches will fail to stop an overpressure condition, the PFD will be the complement of this 1oo2 reliability:

$$PFD = 1 - \text{Dependability}$$

$$\text{PFD}_{1oo2} = 0.001007$$



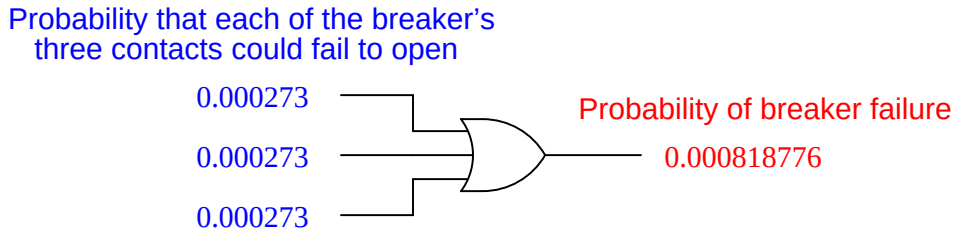
Answer 16

After a failure has been detected in breaker #5, the following circuit breakers need to be tripped in order to isolate breaker #5:

- Breakers #1, #2, #3, and #4 (isolates Bus A from all power sources)
- Breaker #10 (isolates breaker #5 from Bus B)

This protective action cuts power to all loads on the bottom distribution line, while maintaining power (from Bus B) to all other loads.

PFD calculation:



One way to detect a failed breaker is by monitoring the current through it in the "tripped" state. Obviously, a tripped circuit breaker should have no current going through its contacts at all! The question now becomes, how to measure current through the circuit breaker, and this is where the photo proves its value: the numbered cylinders at the base of each insulator bushing on the circuit breaker each houses one current transformer (CT). This is standard on high-voltage circuit breaker construction: each terminal into and out of the circuit breaker has its own dedicated CT to be used for current monitoring, and these current signals may be used to detect a failed breaker condition.

The Socratic Questions on probability may be answered by first organizing the given information on breaker dependability and security (as well as the complementary measures of undependabilty (PFD) and unsecurity, shown in italic font):

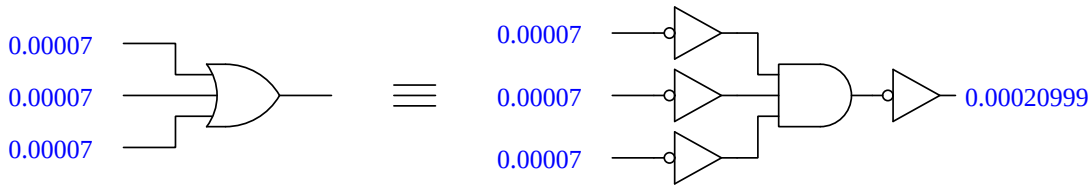
	Breaker told to trip	**Breaker not told to trip**
Breaker trips	0.99918	*0.00007*
Breaker does not trip	*0.00082*	0.99993

In general terms, this is what each of the cells in the table mean:

	Breaker told to trip	**Breaker not told to trip**
Breaker trips	Dependability (RSA)	Un-security
Breaker does not trip	Un-dependability (PFD)	Security

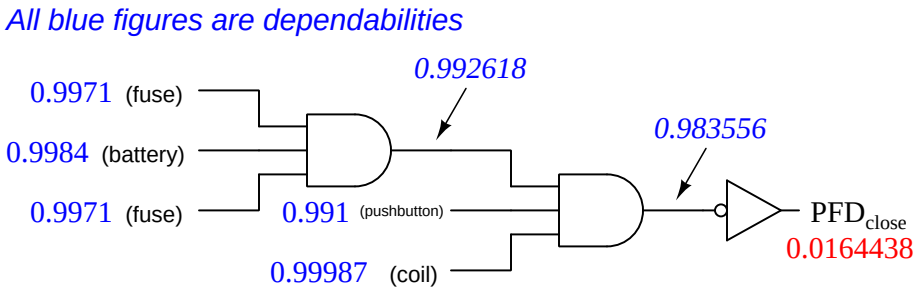
Any given scenario may then be drawn as a logic gate diagram with appropriate values pulled from the table:

→ The probability that the left-hand transmission line will be unnecessarily removed from service (i.e. opened so it no longer carries load current). *(i.e. the probability that either breaker G or J or 1 will trip when it's not supposed to.)*

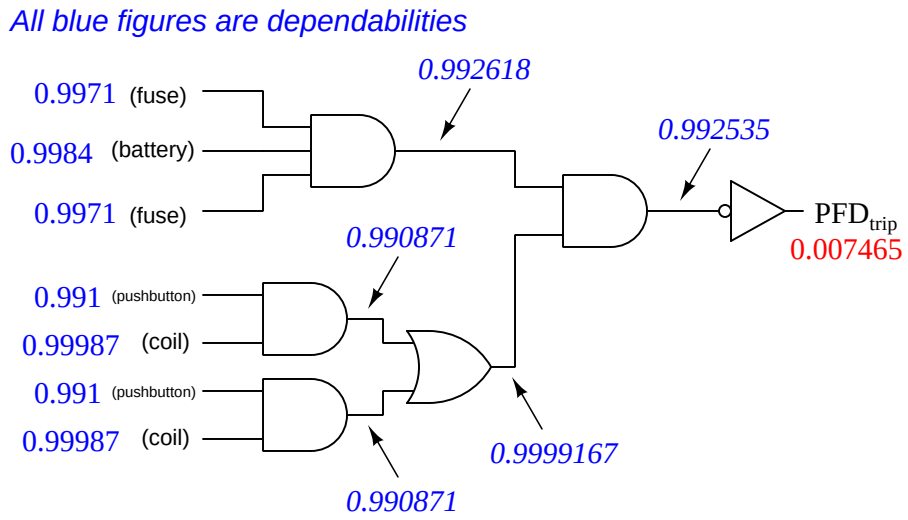


Answer 17

Probability calculation for "closing" PFD using logic symbols:

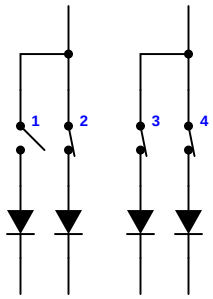


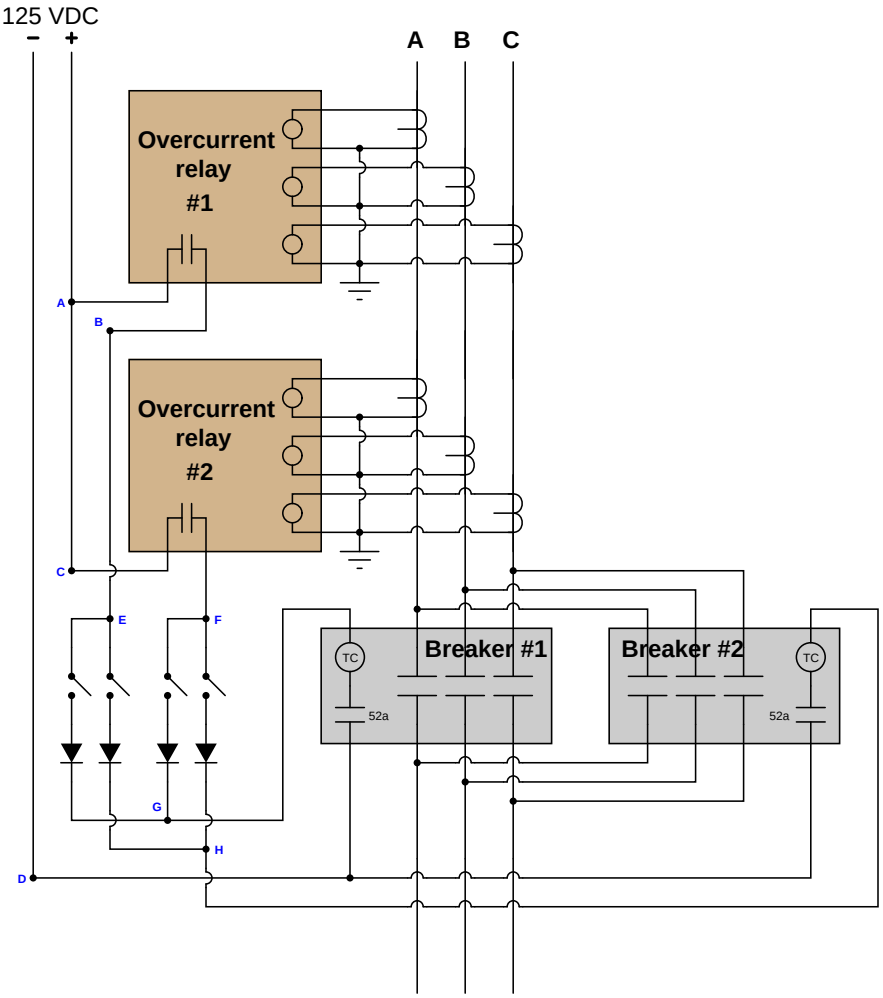
Probability calculation for "tripping" PFD using logic symbols:



Answer 18

Switch positions (#2 through #4 closed, #1 open):





If not for the diodes, trip signal current would "backfeed" in such a way that one relay might end up tripping both circuit breakers even though you only intended it to trip one circuit breaker.

Dependability/PFD calculation: