Safety

Bunker tank at a boiler house. On average, every three years, there is a risk of bunker tank overflow at the boiler house, due to pump and other equipment failures. Cleaning up the environment from the consequences of the overflow costs 25 000 EUR.

Propose a protection circuit using the level sensor in order to prevent tank overflow (price: 200 EUR; fault rate: $2 \cdot 10^{-5}$ $1/h$; dangerous failures (does not work if necessary) and harmless errors (incorrect application) have equal probability $\lambda = \lambda_d + \lambda_h$; sensor performance must be checked once a year). The Mean Downtime Time (MDT) for the deployment of the protection circuit costs 250 EUR.

Calculate the costs in case of boiler equipment failure

- without any protection circuit;
- with 1 sensor in the protection circuit;
- with multi-sensor system (2,3).

Minimize costs of the boiler house in case of failures.

Comments

1 There is no any protection

- failure is a random event;
- average time interval between failures is $t_f =$ .... $years$;
- annual failure probability is $P_f = 1/t_f =$ ....;
- failure causes an accident, accident probability $P_a = P_f$
- accident cost $C_a =$ .... EUR
- annual costs $M_a = P_a \cdot C_a =$ .... EUR

Build a protective circuit (we spend the money for purchases, but will reduce the cost of accident).

2 An ideal sensor

Protective circuit can breakdown:

- sensors are characterized by fault rate $\lambda =$ .... $1/h$;
  - sensor failure is a random event,
  - Mean Time Between Failure $MTBF = 1/\lambda =$ .... $h =$ .... $years$,
  - reliability (probability during the t time) is $R(t) = e^{-\lambda t}$ $/R(0) = 1, R(\infty) = 0/$,
  - probability of failure is $q = 1 - R \approx \lambda t$ if $(q \ll 1)$,
- sensor failure probability per 1 year is $q(1\ y) =$ ....

Then sensor breaks down the protection circuit does not work.

3 Real Sensor - Inspection of protection circuit

Inspection time interval is T

- probability of failure during the T is $q = \lambda T$;
- time instant then failure have happen is a random (which has a uniform distribution at time interval T);
- as a result of sensor failure it is unavailable until the next inspection;
- in case of failure the duration of the unavailability is $T/2$;

- probability to fail on demand during the inspection interval T: $\lambda T \cdot T/2 =$ (failure probability) $\cdot$ (unavailability time), so PFD $= (\lambda T \cdot T/2)/T = \lambda T/2$
- accident happens if during the failure sensor is unavailable, so accident probability $P_a = P_f \cdot$ PFD $=$ (failure probability) $\cdot$ (sensor PFD).

Annual costs:

- in case of accident $M_a \cdot P_f \cdot \lambda_d T/2 = \dots\dots\dots$ EUR
- for sensor $C_s/MTBF = C_s/(1/\lambda) = \dots\dots\dots$ EUR
- $MDT = \lambda_h \cdot T \cdot$ cost......... EUR

4 MooN

"1oo2" - output is ON if at list one input of the two is ON.

$Y = A_1 \vee A_2$ - danger

$\bar{Y} = \bar{A}_1 \& \bar{A}_2$ - there is no danger (pump is working if) (no danger A_1) and (no danger A_2)

Sensors' costs are increased.

"2oo3"?

In case of independent failures

- probability of dangerous failures $P_{df} = q \cdot q$ - remarkably decreased
- probability of non-dangerous failures $P_{hf} = 2q$ - number of downtime increases

Annual costs = accident + sensor + downtime = ... EUR