

Safety

Aim of the work

Probability failure on demand, availability, failure cost

1 Overflow protection circuit

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 20 000 EUR.

Propose a protection circuit using the level sensor in order to prevent tank overflow (price: 150 EUR; failure rate: $4 \cdot 10^{-5}$ 1/h; dangerous failures (dependent) and harmless errors (independent) 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 $C_{\text{idle}} = 300$ EUR.

Calculate the costs in case of boiler equipment failure

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

Minimize costs of the boiler house in case of failures.

Comments

2 There is no any protection

- Failure is a random event;
- Average time interval between failures is $t_f = \dots\dots\dots$ years;
- Annual failure rate is $P_f = P_a = 1/t_f = \dots\dots\dots$;
- Accident cost $C = \dots\dots\dots$ EUR
- Annual costs $C_{\text{annual}} = P_a \cdot C = \dots\dots\dots$ EUR

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

3 An ideal sensor

Protective circuit can breakdown:

- Sensors are characterized by failure rate $\lambda = \dots\dots\dots \left[\frac{\text{failures}}{\text{year}} \right];$
 - sensor failure is a random event,
 - Mean Time Between Failure MTBF = $1/\lambda = \dots\dots\dots [h] = \dots\dots\dots [years],$
 - reliability (probability during the t time) is $R(t) = e^{-\lambda t} \quad /R(0) = 1, R(\infty) = 0/,$
 - probability of failure is $q = 1 - R ,$
- Sensor failure probability per 1 year is $\text{PFD}_{\max} = \dots\dots\dots$

Then sensor breaks down the protection circuit does not work.

4 Real Sensor - Inspection of protection circuit

Inspection time interval is T

- Probability of failure during the T is $\text{PFD}_{\max} = 1 - e^{-\lambda T};$
- 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 $T/2;$
- Average probability to fail on demand during the inspection interval T : $\text{PFD}_{\text{avg}} = \lambda T/2$
- Accident happens if during the failure sensor is unavailable, so accident probability $P(A_1 \& A_2) = P(A_1) \cdot P(A_2) \implies P_a = P_f \cdot \text{PFD}_{\text{avg}} = (\text{failure probability}) \cdot (\text{sensor PFD}).$

Annual costs:

- In case of accident $C_{\text{accident}} = C \cdot P_a = \dots\dots\dots \text{ EUR}$
- For sensor $C_{\text{sensor}} = C_s/\text{MTBF} = \dots\dots\dots \text{ EUR}$
- $C_{\text{MDT}} = \lambda_h \cdot T \cdot C_{\text{idle}} \dots\dots\dots \text{ EUR}$
- Planned down time for maintenance

5 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.

$$PFD_{avg_{1oo2}} = \frac{(\lambda T)^2}{3}$$

$$PFD_{avg_{1oo3}} = \frac{(\lambda T)^3}{4}$$

"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

$$PFD_{avg_{MooN}} = \frac{\frac{N!}{(M-1)!}}{(N-M+1)!} \frac{(\lambda T)^{(N-M+1)}}{(N-M+2)} \quad (1)$$

$$PFD_{avg_{NooN}} = N\lambda \frac{T}{2} \quad (2)$$

Annual costs = accident + sensor + planned downtime + downtime because of failure =
 EUR