Probability in control systems

A control system or device is deemed to be safety related if it provides functions which significantly reduce the risk of a hazard. At Invensys control systems I have been working on the Kashagan project.

The Kashagan project is an oil plant in Kazakhstan estimated to produce 35 billion barrels, the size of the plant requires obvious high intensity safety control systems, as the impact of any hazard here would be significant to the whole world, probability calculations are of great importance to Invensys to analyse any risk.

The table on the next page will explain how the below values are calculated.

MTTR = mean time to repair

(this is our immediate independent variable which is improved by training, or more immediate repair supplies.)

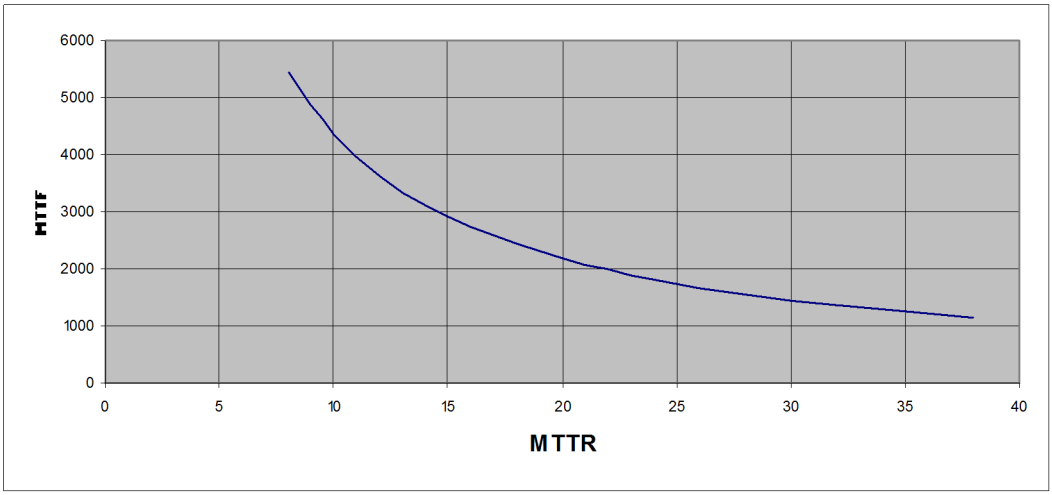
MTTF = mean time to Fail

(this is our dependant variable)

This table shows how as the time to repair increases the more likely a fail will happen. The results are summarized by the graph below.

MTTR	MTTF
8	5458.123536
10	4366.595013
12	3638.909292
14	3119.133763
16	2729.302148
18	2426.099771
20	2183.53786
22	1985.078119
24	1819.694996
26	1679.755438
28	1559.807243
30	1455.852137
32	1364.891422
34	1284.631964
36	1213.290226
38	1149.458144

A graph to show how the mean time to repair effects the likelihood of a fail in years



MTTR (Mean time to repair)			8
Component			Component Failure Rate
PSU for copper switch			0.01752
Copper Switch			0.01639
PSU for FO switch			0.01752
FO Switch			0.02985
TCM Failure Rate			0.03
Loop Total Fail rate /Year	FR	1-(P(s)*P(s)*P(s)) (1)	0.106527902
Probability of being Failure per MTTR Hour Period	P(Fail)	FR * MTTR / 8760 (2)	9.72858E-05
P(both fail in one 8 hour time slot)	P(both fail)	1- (P(s)^2) - 2(P(s) x P(f)) (3)	9.46452E-09
P(at least one dual loop faliure per year)	P(dual fail) per year	1- (1-P(both fail))^(8760/MTTR) (4)	1.03636E-05
Instances	N		17
Probability of Loop failure in 1 year	LFR	1 - (1 - P(DF)) ^ N (5)	0.000176166

1) First we must work out the probability that at least one component fails, this is 1 - probability of total success which we can work out by multiplying the probability of success for all the components where the probability of success is 1 - P(f)

The next part of the problem comes that each loop that contains all these components has a back up loop, so if any one component fails it will switch to the second loop. Since each fail takes on average 8 hours to repair, given by the MTTR, we can assume a dual loop failure will only occur if there is a failure on both loops within the same 8 hour period.

2) So from this the first step is to work out the probability of a loop failing within 8 hours, which is simply, Failure Rate, worked out in step 1 multiplied by the MTTR and then divided by the number of hours in a year which Is 8760

3) The third step is to work out the probability of two loops within the dual loop failing within the same 8 hour period. The possible combinations of success and failure is
P(s) x P(s)
P(f) x P(s)
P(s) x P(f)
P(f) x P(f)
All of these combinations sum to 1, we can denote from this, the probability of failure in both loops is

1 - [P(s) x P(s)] - [P(f) x P(s)] - [P(s) x P(f)] = [P(f) x P(f)]

4) Once we have worked out the probability of two loops failing within the same 8 hour period we can work out the probability of two loops failing in a year by using a similar formula used in step 1.
1 - the probability of success ^ (8760/MTTR) = 1- (1-P(both fail))^(8760/MTTR)

5) As we are told there are 17 dual loops in a system we must work out the probability that at least one dual loop fails, similarly 1 - the probability of success ^ (17) = 1 - (1 - P(DF)) ^ N

Add Common mode Failure factor	TRFx	TFR * 1.04 (Assume 4%)	(6)	0.000183213
MTTF (Years)		1/P(dualFail)	(7)	5458.123536

6) we must take into consideration any external factors, we have assumed each probability is independent, but as this is unrealistic the standard factor or error to include is 4% on the total. So this step just multiplies the probability by 1.04

7) The Final step gives us, from the probability, how long until we would expect a dual loop failure.

This value is a good evaluation of the system and can provide information on how reliable we expect the system to be, if the value is too low further action will be taken to increase the expected reliability.