Reliability Analysis for Safety Grade PLC(POSAFE-Q)

KyungChul Choi [a†], SeungWhan Song[a], GangMin Park[a], SungJae Hwang[a]

[a] POSCO ICT Co. R&D center,
Korea Techno-complex 126-16,
5-ka, Anam-dong, Sungbuk,
Seoul,
Republic of Korea

Abstract. Safety Grade PLC(Programmable Logic Controller), POSAFE-Q, was developed recently in accordance with nuclear regulatory and requirements. In this paper, describe reliability analysis for digital safety grade PLC(especially POSAFE-Q). Reliability anlaysis scope is Prediction, Calculation of MTBF(Mean Time Between Failure), FMEA(Failure Mode Effect Analysis), PFD(Probability of Failure on Demand).

1. Introduction

In this paper, describe reliability analysis for digital safety grade PLC which developed with the aim to use the operating nuclear power plants and new plants by POSCO ICT co., POSAFE-Q consist of the Sub Rack, power modules, processor modules, communication modules, digital input / output module (DI / DO), analog input / output modules (AI / AO), pulse counter module, TC (Thermocouple), RTD (Resistance Temperature Detector), Local Repeater.

2. Methods and Results

Reliability evaluation is Mean Time Between Failure (MTBF) of module which quantitative estimation and Probability of Failure on Demand (PFD) which qualitative estimation.

Mean Time Between Failure(MTBF) was predicted failure rate of parts based on [4], calculated Mean Time Between Failure(MTBF) of 27 modules consisted of POSAFE-Q, calculated Probability of Failure on Demand(PFD) of POSAFE-Q(included processor module) based on [7].

2.1 MTBF(Mean Time Between Failure)

In order to predict failure rate of POSAFE-Q, applied method is the Part Stress Method based on [4]. Assumption which applied as follow:

- Lifetime of the part follows an exponential distribution. (Constant failure rate)
- All parts of a module is connected in series.
- Each component is statistically independent.

Predicted failure rate (λ_p) of the unit or system on Part Stress Method is as follow,

$$\lambda_p = \sum_i \lambda_{g_i} \pi_{Q_i}$$

(λ_i: basic failure rate of part i, Q_i: Quality factor of part)

In addition, temperature 30 □ and 50 □, 50% and 80% of the electrical stress was applied for. Under these conditions, the MTBF of each module, which was distributed in 8.4 years to 58 years, under normal conditions (temperature 30 □, the electrical stress 50%) showed a minimum of 18 years MTBF.

Table I. Failure rate prediction result from change of environmental temperature and electrical stress

Module	Temp. 30℃		Temp. 50℃	
	Elec. Stress (50%)		Elec. Stress (80%)	
	Failure Rate (FPMH)	MTBF (Yr)	Failure Rate (FPMH)	MTBF (Yr)
BUS	1.9194	60.30	3.2192	35.95
POWER	3.8051	30.42	8.1078	14.28
CPU	4.9406	23.43	13.4871	8.58
Optic Comm.[a]	3.4513	33.54	8.2956	13.95
230Vac DI	4.4104	26.24	9.6290	12.02
125Vdc DO	3.3449	34.60	6.7739	17.09
SSR DO	4.7280	24.48	8.0844	14.32
24Vdc DI	5.4222	21.35	11.3925	10.16
24Vdc DO	4.0468	28.60	8.1106	14.27
RELAY DO	3.3067	35.00	6.9785	16.59
AI	4.0036	28.91	12.7011	9.11
RTD	3.2382	35.74	8.4320	13.73
TC	3.0868	37.50	8.3490	13.86
AO	3.6138	32.03	9.8364	11.77
PULSE Cnt.[b]	6.1079	18.95	12.7229	9.10

[a] Optical Communiction Module using fiber optic cable
[b] High Speed Pulse Counter Module

2.2 FMEA(Failure Mode Effect Analysis)

In case of FMEA, separate Safe Failure and Dangerous Failure as follow Fig.1 about failure, and divide each separated failure by diagnosis as possible and diagnosis as impossible. We examined the degree of failure mode effect from separation and performed evaluation about failure detection method.

.

Execution of FMEA was carried out following the procedure.

1) Prepare for related material of components
2) Identify feature of components
3) Determine decomposition level of components
4) Make a functional block
5) Identify the type and cause of failure
6)Quantitative Analysis(Severity/Occurrence/Detection)
7) Calculate RPN (Risk Priority Number)
8) Safe Assessment
9) Check the problem Countermeasures

Table II. FEMA of POSAFE-Q modules

LRU Description	TFR ($F/10^6hr$)	SFF	DCS	DCD	tCE	tGE	PFD
CPU	4.6622	1	1	1	0.5	0.5	0.004627
COMM.	3.1968	1	1	1	0.5	0.5	1.0264
DI	5.1626	1	1	1	0.5	0.5	2.1107
DO	3.4445	1	1	1	0.5	0.5	1.6653
AI	3.7224	1	1	1	0.5	0.5	1.6931
AO	3.4951	1	1	1	0.5	0.5	1.6308

* TFR: Total Failure Rate
DCS: Diagnostic Coverage Safe
DCD: Diagnostic Coverage Dangerous
SFF: Safe Failure Fraction
tCE: Channel equivalent mean down time
tGE: System equivalent down time

2.3 PFD (Probability of Failure on Demand)

Failure defined [7] is classified Safe Failure and Dangerous Failure as follow Fig.1. Safe Failure is classified Detected Safe Failure and Undetected Safe Failure. Likewise, Dangerous Failure is classified, as a dangerous failure (Dangerous Failure) can be detected and cannot even be classified.

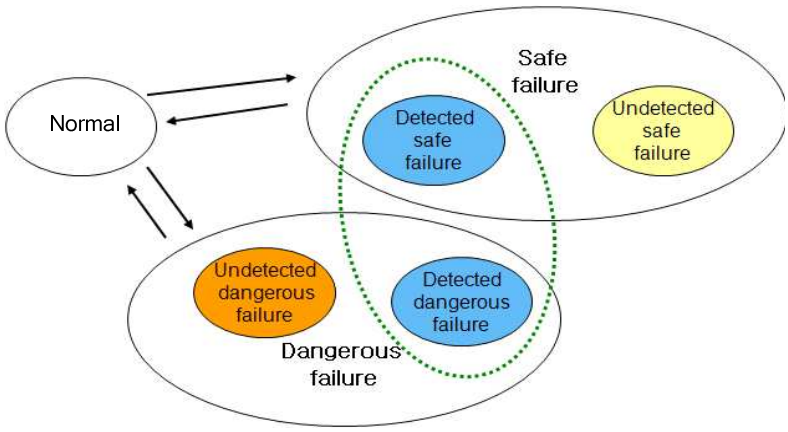

Fig. 1. Failure defined in [7]

Structure of POSAFE-Q is serial structure (1oo1 structure) for other modules except for redundant processor module (1oo2 structure)

Table III. Calculation of PFD (Failures / 10^6hr)

LRU Description	λ_S	λ_{SD}	λ_{SU}	λ_{SD}	λ_{DD}	λ_{DU}
CPU	0.9662	0.9662	0	3.696	3.696	0
COMM.	0.9434	0.9434	0	2.0528	2.0528	0
DI	0.9412	0.9412	0	4.2214	4.2214	0
DO	0.114	0.114	0	3.3305	3.3305	0
AI	0.3362	0.3362	0	3.3862	3.3862	0
AO	0.2335	0.2335	0	3.2616	3.2616	0

* λ_S: Safety Failure Rate
  λ_{SD}: Safe Detected Failure Rate
  λ_{SU}: Safe Undetected Failure Rate
  λ_{SD}: Dangerous Failure Rate
  λ_{DD}: Dangerous Detected Failure Rate
  λ_{DU}: Dangerous Undetected Failure Rate

In case of POSAFE-Q consisted of 27 modules, PFD is sum of PFD for 1oo1 structure of 26 modules and PFD of 1oo2 structure (CPU module). In other words,

$$PFD_{POSAFE-Q} = \sum_{i} PFD_i + PFD_{NCPU-2Q} = 4.88 \times 10^{-5}$$

(i= 1oo1 structure of all modules)

3. Conclusions

PFD(Probability of Failure on Demand) of POSAFE-Q, including redundant processor modules ,was calculated to be 4.88 X 10^{-5}. It is mean that occur 1 time failure about 20,000 times on demand. Numerically, the reliability of POSAFE-Q is equivalent to the category top-level SIL 4 of SIL (Safety Integrity Level) according to classification criteria of [7]. The breakdown of these results, each module can be detected a large part of failure always. This system structure make very low about dangerous failure rate for does not detect. In particular, compare the failure rate of each module, failure rate of the redundant processor module was relatively high, but can be decreased much lower possibility of failure occurrence on demand by redundant.

A few assumption for the calculation when reliability analysis, but it is reasonable assumption realistically, the assumption significantly affect the result of reliability is not excessive assumption. The results of PFD, it is consider that POSAFE-Q are equipped with sufficient reliability can be applied to the safety systems of a NPP I & C system.

REFERENCES

[1] 10 CFR 50, App.A, General Design Criteria for Nuclear Power Plants.
[2] 10 CFR 50, App.B, Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants.
[3] USNRC Reg. Guide 1.152, Criteria for Programmable Digital Computers System Software in Safety Related Systems of Nuclear Power Plants, Jan. 2006.
[4] MIL-HDBK-217F (Notice 2), Reliabilty Prediction of Electronic Equipment, 1995
[5] IEEE Std 352, Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Safety Systems, 1987.
[6] IEEE Std 603, Standard Criteria for Safety Systems for Nuclear Power Generating Stations, 1998.
[7] IEC 61508, Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems, IEC, 1998.
[8] POSAFE-Q-00000-D-202-1, POSAFE-Q System Require ment Specification, 2009.04.13.