# Common Cause Failure: Enhancing Defenses against Root Cause and Coupling Factor

Poorva P. Kaushik [a,b*], Sok Chul KIM [a*]
[a] *Korea Institute of Nuclear Safety, 62 Kwahak-ro, Yuseong, Daejeon, Korea, 34142*
[b] *Korea Advance Institute of Science and Technology, 291 Daehak-ro, Yuseong-gu, Daejeon, Korea*
[*] *Corresponding author: jupiter@kins.re.kr, poorvakasuhik@gmail.com*

## 1. Introduction

A Common Cause Failure (CCF) event refers to a specific class of dependent events that result from co-existence of two main factors: Susceptibility of components to fail or become unavailable due to particular root cause of failure, and coupling factor (or coupling mechanism) that creates the condition for multiple components getting affected [1].

PSA (Probabilistic Safety Assessment) results and operating experience of Nuclear Power Plants (NPPs) have demonstrated that dependent events such as CCF events are major contributor to risk during operation.

From cost-benefit consideration, putting significant design modifications in place to prevent CCF would not be desirable in terms of risk management and, regulatory effectiveness and efficiency. The present paper proposes development of an easy to implement practical defense strategy against coupling factors and common root causes. Explicit defense strategy can be put in place by the development of CDM (Cause-Defense Matrix) and CFDM (Coupling Factor -Defense Matrix).

In the present study, CDM and CFDM for generic Emergency Diesel generator (EDG) are developed. It is proposed that the incorporation of these defense strategies will result in modification of Applicability Factor of the Event Impact Vector by the factor of 0.25. Proposed EDG CDM (Cause-Defense Matrix) and CFDM (Coupling Factor -Defense Matrix) provides effective and efficient measures for reducing risk contribution of EDG to CDF in terms of cost-benefit consideration.

## 2. Methods and Results

PSA results of a NPP infer that the Loss of Offsite Power event would be a significant contributor to CDF. Thus, it is desirable to secure high reliability of emergency power supply system with improving defense capability against CCF of EDG effectively and efficiently.

The identification of the vulnerability to CCF at NPP requires comprehensive review of the operating experience of NPPs.

Following section denotes summary of literature review of operating experience of EDG and outlines proposed CDM and CFDM of EDG.

### *2.1 Literature Survey for Insights about EDG Failure*

NUREG/CR-6819 [2] gives CCF events insights for EDG. Event Summary of 138 events (from 1999-2000) given in this report was reviewed and system wise contribution is depicted in Fig 1. It was observed that the highest number of events occurred in the instrumentation and control sub-system (41 events or 30 percent) followed by the cooling, engine, fuel oil, and generator sub-systems. Last four subsystems comprised over 50 percent of the EDG CCF events. The battery, exhaust, and lubricating oil subsystems were minor contributors.

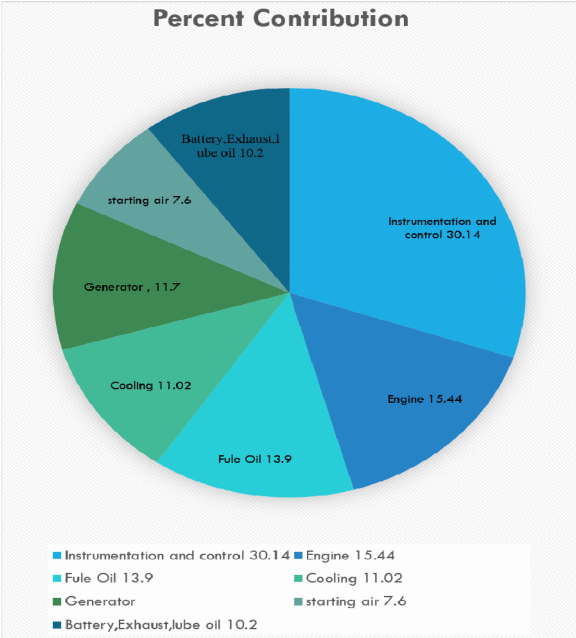


Fig. 1 System wise distribution of Failure of EDG (%)

It was also observed that shortcoming in design is the leading coupling factor (66 events or 48 percent) followed by maintenance (39 events or 28 percent) which accounted for the majority of the remaining events. The environmental, hardware quality and operation were contributing to a lesser degree. Major root causes contributing to above CCF events are summarised in Table I.

Table I: CCF proximate causes for EDG failure

| CCF Cause | Percentage |
|---|---|
| Design/Construction/Installation/Manufacturing inadequacy accounted. | ~33% |
| Internal to Component faults accounted. | ~30% |
| Human error accounted. | ~22% |
| External Environment and the other proximate cause categories assigned to the EDG component. | ~15% |

### *2.2 Development of Defense Matrix*

The explicit defense strategy was developed for EDG based on the insights gained from literature review. There are three methods of defense against a CCF

a) Defense against root cause.
b) Defense against coupling factor.
c) Defense against both root cause and coupling factor.

The defense strategy against failure root causes will reduce the number of individual failures and the defense strategy developed against coupling factor will eliminate the relationship between the failures. However, the most comprehensive strategy is developing defense against both root cause and coupling factor. Thus, both CDM and CFDM were developed for generic EDG. Fig. 2 Illustrates the CDM for each sub system of EDG. The design control, use of qualified equipment, testing and preventive maintenance programs, procedure review, and personnel training quality Control etc. are the main defenses employed.

Fig. 3 demonstrates the CFDM and lists various strategies that can be adopted against each system of EDG for reduction of CCF due to coupling factors. Typical defenses adopted against coupling factor are diversity (functional, equipment, staff), physical or functional barriers (spatial separation physical protection, interlocks removal, or administrative control on cross ties), and testing and maintenance policy (staggered testing, staggered maintenance).

The defenses adopted are feasible and easy to implement for both CDM and CFDM.

| Selected Failure Mechanism | Procedural Control/ General Administrative Control | | | Maintenance/Operational Practices | Design Features |
|---|---|---|---|---|---|
| | Configuration Control | Maintenance/Operating Procedure | Test Procedures | | |
| **Instrumentation Control**<br><br>Relay Failure due to dust deposition<br>Failure of relay sockets due to high vibration<br>Resistor failure in Governor<br>Governor out of adjustment | -Closure of panel doors where relay are mounted. | -Special Focus on Relay Contact Cleaning in Maintenance Procedure<br>-Improved maintenance practice of governor.Flush the governor in order to cleaning out contaminated oil. | -Vibration measurement of the structure on which relays are mounted to be done on regular basis and compared with baseline data. | -Program for aging management of internal instrumentation and control components including removing the part as early as there design age is over. | -Dust Covers with seals on relay Cabinet<br><br>-Improved and Clean Ventilation of relay room<br><br>-Improved installations of relays |
| **Starting Air System**<br><br>-Corrosion products in Air start system<br>-Air start Receiver leakage<br>-Air Start system valved out | -Strict and Improved control of -configuration of valves of Air start system | -Reviewed and Improved hold Test of Air receiver | -To include in the Test procedures of the action of reverting the valves which were closed for auto start test of compressors. | -In Daily Routines ,<br>- Monitoring of dew point of dry air,<br>-Check for any hissing sound during field round to get early warning of impending leak and Perform in routine leak tightness test through soap solution. | -Instrumentation to note the dew point to prevent corrosion<br>-Material of construction of receiver and piping of air system compatible with air e.g. have SS lining.<br>-Provision of Limit Switch in the valves to get early notification of inadvertent closure. |
| **Cooling:**<br>Corrosion in jacket cooling system<br>Improper line up of cooling water system<br>Aquatic organism in service water system | -Strict and Improved control of configuration of cooling System. | -Revised Maintenance procedure of water cooling draining and filling procedures. | -To include in Test Procedure to add recommended quantity of chemicals before test and give samples after test.<br>-Proper flushing of sampling bottles before sampling. | -Addition of Corrosion Inhibitors in jacket cooling water system.<br>-Enhanced sampling of Jacket cooling water system.<br>-During PM schedule proper condition monitoring of jackets for any fungal growth to be ensured. | -Review of vulnerable point is cooling water system that are prone to air ingress<br>-Design review of Sampling provision to get representative sample. |
| **Fuel Oil System:**<br>-Water/sediment/fungus in Oil<br>-Fuel Pump strainer blockage<br>-Fuel oil Spurious draining/wrong valve configuration<br>-Fuel Oil pump priming<br>-High Vibration in Piping | -Strict and Improved control of configuration of valves of Fuel Oil System by formal methods like : Order to Operate system with temporary field tags and direct accountability, | -Improved maintenance of Pump Suction Strainers.<br>-Self cleaning strainers can be installed. | -Include in TP to measure Vibration of fuel oil system piping during EDG running condition | -Regular draining of water and sediments from the tanks .<br>-Enhanced Sampling of Fuel Oil.<br>-Include in BSD schedule for monitoring of fuel oil storage tank internals for any fungal growth/ sediment deposition. | -Incorporation of Drains in Fuel Tank and lower most point of fuel oil piping.<br>-Incorporation of Syphon in fuel oil suction line to prevent loss of prime.<br>-Venting of Fuel Oil Storage tank with syphon to prevent atmospheric ingress of moisture. |
| **Engine:**<br>-Turbocharger fan failure due to bad quality<br>-Inadequate lubrication of pistons due to design deficiency | -Plugging of valves in drain line as in case of inadvertent opening of drain valve plug will prevent draining. | -Close visual inspection of piston and other lubricated parts to catch the early sign of degradation | -To include in TP regarding turbocharger abnormal noise checking | -Sampling of Engine lubricating oil on regular basis for identifying traces of metal in oil/ wear particles. | -Strict quality assurance during manufacturing and installation.<br>-Revisit the design to improve splash lubrication of engine |
| **Lube oil System:**<br><br>-Contamination of oil due leak in lube oil cooler<br>-leak of lube oil due to failure of check valve | -Drain valves of lube oil system to be kept chain locked to avoid inadvertent draining. | -Operating procedure to carry out isolation and normalization of heat exchangers such that at no pint pressure on water is more that that at oil side. | -Include in TP to check the leak around check valve during DG running as leak will exist only during DG running. | -Correct Pressure Maintenance across the Plates of heat exchanger during draining/isolation to prevent cooling water ingress to lube oil. | -Excessive difference in pressure of process water and lube oil cooler to be avoided.<br>-If pressure difference is unavoidable higher pressure should be of lube oil system. |
| **Breaker:**<br>-Output breaker failed to close due to oxidation/pitting of contacts<br>-Malfunctioning of trip lockout relay<br>-Out breaker did not closed due to deformed spring retainer | - | - | -Improved maintenance practice and training of personnel. | -Spring retainer inspection to be included in the PM schedule.<br>-Breaker contacts to be checked during PM for oxidation products. | -Improved ventilation of breaker room |

Fig. 2 Cause - Defense Matrix

| Selected failure mechanism | Diversity | Barrier | | Testing and maintenance | |
|---|---|---|---|---|---|
| | Functional/Equipment/Staff | Spatial Separation | Removal of cross ties | Staggered testing | Staggered Maintenance |
| **Instrumentation Control :**<br>-Relay Failure due to dust deposition<br>-Failure of relay sockets due to high vibration<br>-Resistor failure in Governor<br>-Governor out of adjustment | -Use of Numerical relays and Electromagnet relay.<br>-Relay Bought from bought vendors | -Spatial Barrier among relays as much as possible like relay performing same function in different cabinets. | - | - | - |
| **Starting Air System**<br>-Corrosion products in Air start system<br>-Air start Receiver leakage<br>-Air Start system valved out | -Compressed Air Dryers working on different principle<br>-Silica Gel Desiccant dryer<br>Membrane Dryer (Nitrogen membranes)<br>-Peer review in carrying out Isolation for system Important to safety. | - | -Cross tie valve between air receiver of two tanks need not be removed but strict administrative control and enhanced maintenance of tie valve .<br>-Additional indication of tie valve position in MCR | - | -Staggered Maintenance of Air receiver tanks and Tie valves |
| **Cooling:**<br>-Corrosion in jacket cooling system<br>-Improper line up of cooling water system<br>-Aquatic organism in service water system | -Chemical Addition in Jacket cooling system from different sources may be tried<br>-Diversity in Staff carrying out the Isolation and preparing the permit for isolation.<br>-Checking of DM water quality at two different Chemical laboratories. | - | -Removal of cross ties between the make up water to jacket cooling water system | - | -Staggered maintenance of Cooling water system |
| **Fuel Oil System :**<br>-Water/sediment/fungus in Oil<br>-Fuel Pump strainer blockage<br>-Fuel oil Spurious draining/wrong valve configuration<br>-Fuel Oil pump priming<br>-High Vibration in Piping | -Staff Diversity in testing and maintenance and sampling<br>Checking of oil samples at two different labs. | -Different Location of fuel oil storage tank of different DGs. | -Removal of cross ties between fuel oil system or strict administrative control of tie valves . | -Staggered Testing of Fuel oil system. | -Staggered Maintenance of Pump Suction and sampling of fuel oil |
| **Engine:**<br>-Turbocharger fan failure due to bad quality<br>-Inadequate lubrication of pistons due to design deficiency | -Diversity in staff for manufacturing ,installation and maintenance. | - | - | - | -Staggered maintenance |
| **Lube oil System:**<br>-Contamination of oil due leak in lube oil cooler<br>-leak of lube oil due to failure of check valve | -Spring operated and power operated check valves in fuel oil pipe line at vulnerable points . | | | | -Staggered Maintenance of Heat Exchanger |
| **Breaker:**<br>-Output breaker failed to close due oxidation/pitting of contacts<br>-Malfunctioning of trip lockout relay | -Diversity in lockout relay can be considered. | -Spatial Barrier among breakers of Different EDGs. | - | Staggered testing | -Staggered maintenance |

Fig. 3 Coupling Factor - Defense Matrix

### *2.3 Modelling of CCF event in Probabilistic Safety Assessment* [1]

To quantify the CCF events in PSA various Parametric Model (such as alpha factor, beta factor and multiple greek letter methods) are proposed in literature. CCF parameter estimation is done through industry based generic data. Since the CCF events are rare therefore plant specific assessment of CCF event frequencies is statistically insignificant.

Generic identification of these parameters is carried out by identification of all CCF events. These CCF events are then classified according to the level of impact of events by identifying an "Event Impact Factor" for each event. For a component group of size m, the Event Impact Vector has (m+1) elements. A CCF event of k component will have $(k+1)^{th}$ element of Event Impact Vector as one otherwise zero. In case of EDG component group of size 2, possible Event Impact Vectors are the following:

a) [1,0,0] : No component failed
b) [0,1,0]: Only one component failed.
c) [0,0,1]: Two components failed due to CCF

The parameters of the alpha-factor model "$\alpha_k^{(m)}$" denotes the fraction of the total frequency of failure events that occur in the system that involve the failure of *k* components due to a common cause in a *m* component system. The parameters for alpha factor model are estimated from identified Event Impact Vectors by the co-relation given below.

$$\alpha_k^{(m)} = n_k / (\Sigma n_j) \qquad (1)$$

Where,
$n_k$ = total number of basic events involving failure of k similar components.
$n_j$ = the sum of the *jth* element of the impact vector, over all events

Generic value of alpha factor of two EDG system are : $\alpha_1^{(2)} = 0.953$ and $\alpha_2^{(2)} = 0.047$

*2.4 Parameter re-estimation [1]*

The generic CCF parameters have been developed with the review of generic plant data. However with the incorporation of defenses as per CDM and CFDM discussed in section 2.2, the plant specific performance will differ. The applicability of generic CCF parameter has to be modified for NPP with these strengthened defenses. Modified CCF Parameter can be calculated by calculating Modified Specific Event Impact Vector ($I_r$) given by:

$$I_r = \mathbf{r} * I \quad (2)$$

Where, $r = r_1 * r_2$
$r_1$ is measure of applicability of root cause.
$r_2$ is measure of applicability of coupling factor.

Strength of EDG system defense against the root cause and coupling factor of the event as compared with generic EDG is the basis of re-estimating $r_1$ and $r_2$. On the scale of zero to one, zero strength results in no failure and strength of unity denotes no change in defense. The values of $r_1$ and $r_2$ based on the strength of defense of target system [ref. 1] with the original /average plant are discussed in Table II.

Table II: Applicability factors based on defenses applied. [ref.1]

| Strength of Defense in Comparison to Average Plant | Root Cause ($r_1$) | Coupling Factor ($r_2$) |
|---|---|---|
| Complete Defense | 0 | 0 |
| Superior Defense | 0.1 | 0.1 |
| Moderately Better Defense | 0.5 | 0.5 |
| Weaker or no defense | 1 | 1 |

Conservatively taking the strength of defenses proposed as "Moderately better defense" against root cause and coupling factor ($r_1 = r_2 = 0.25$), the modified Application specific impact vector will be, $I_r = 0.25$ I.

Estimation of plant specific Alpha factor from the revised Impact vectors requires the use of software code. However, Alpha factor if subjectively estimated i.e. by multiplying the generic alpha factor with applicability factor would result in $\alpha_2$ as 0.01175 and $\alpha_1$ as 0.98825.

## 3. Conclusions

The aim of this study was to propose feasible defenses against CCF from cost benefit consideration to enhance the safety. This study provides the CDM and CFDM of EDG. Defenses employed against cause and coupling factor can be easily employed in operation and maintenance programme of NPP and are not an additional cost burden. Such enhancement of defense against the CCF can give a modest improvement in CDF. This approach is specifically helpful in plants that are already under operation and significant modifications are not economically feasible.

## Acknowledgement

This research paper was made possible through the help and support by Korea Institute of Nuclear safety. Sincere gratitude is also hereby extended to Dr. Hyun Gook Kang, KAIST for his unwavering guidance.

## REFERENCES

[1] NUREG/CR-5485 Guidelines on Modeling Common-Cause Failures in Probabilistic Risk Assessment.
[2] NUREG/CR-6819 Common-Cause Failure Event Insights Volume 1 Emergency Diesel Generator, Idaho National Engineering and Environmental Laboratory.