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

Poorva Kaushik and Sok Chul Kim*

*Korea Institute of Nuclear Safety
Department of Nuclear and Quantum Engineering
Korea Advanced Institute of Science and Technology (KAIST)

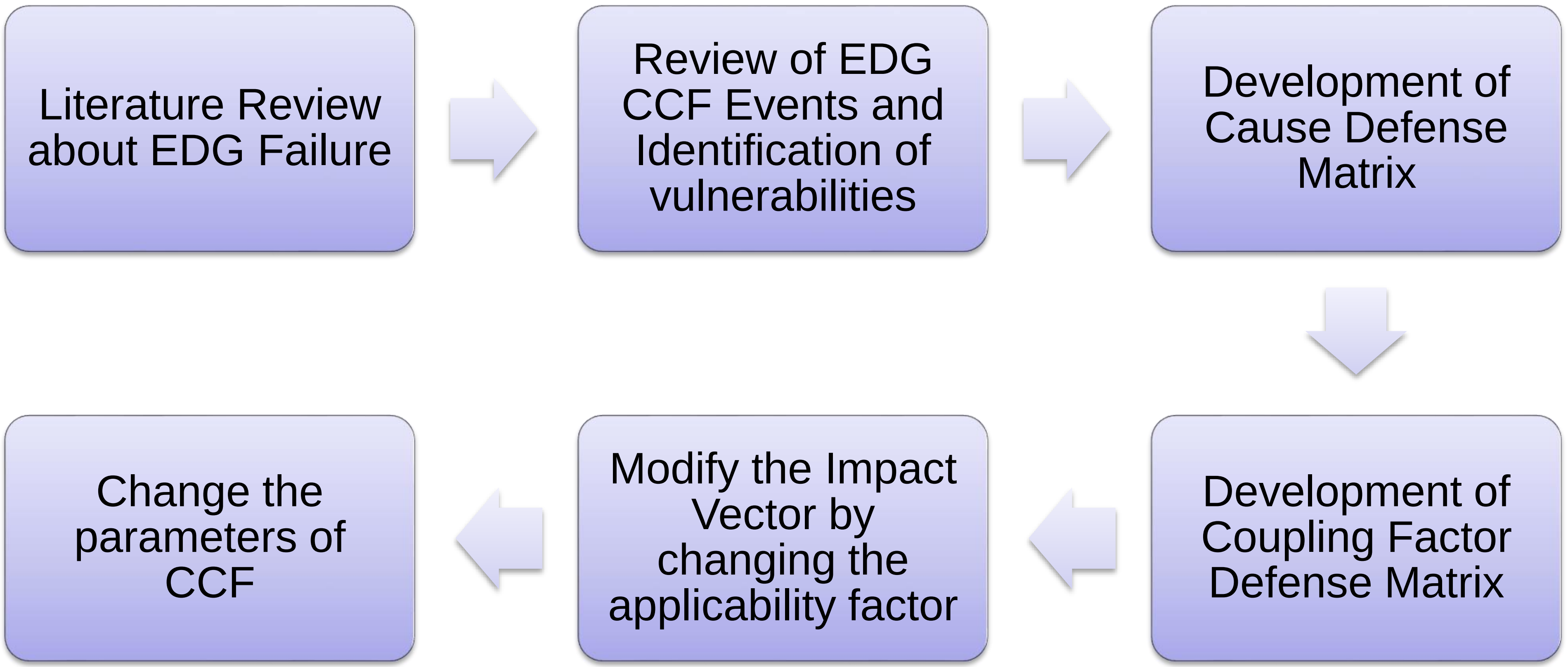
October 27, 2016

Contents

Introduction

- PSA results of NPPs have demonstrated CCF events are major contributor to risk during operation.
- CCFs results from co-existence of two main factors :
  - ✓Susceptibility of components to fail or become unavailable due to particular root cause of failure, and
  - ✓A coupling factor that creates the condition for multiple components getting affected.
- From cost-benefit consideration, putting significant design modifications in place to prevent CCF is desirable
- Study proposes development of an easy to implement practical defense strategy against coupling factors and common root causes.
- CDM and CFDM for EDG are developed to provide effective and efficient measures for reducing risk contribution of EDG to CDF in terms of cost-benefit consideration.

Outline of Study



Literature Review

Following is the root causes and coupling factors distribution resulting in CCF of EDG events

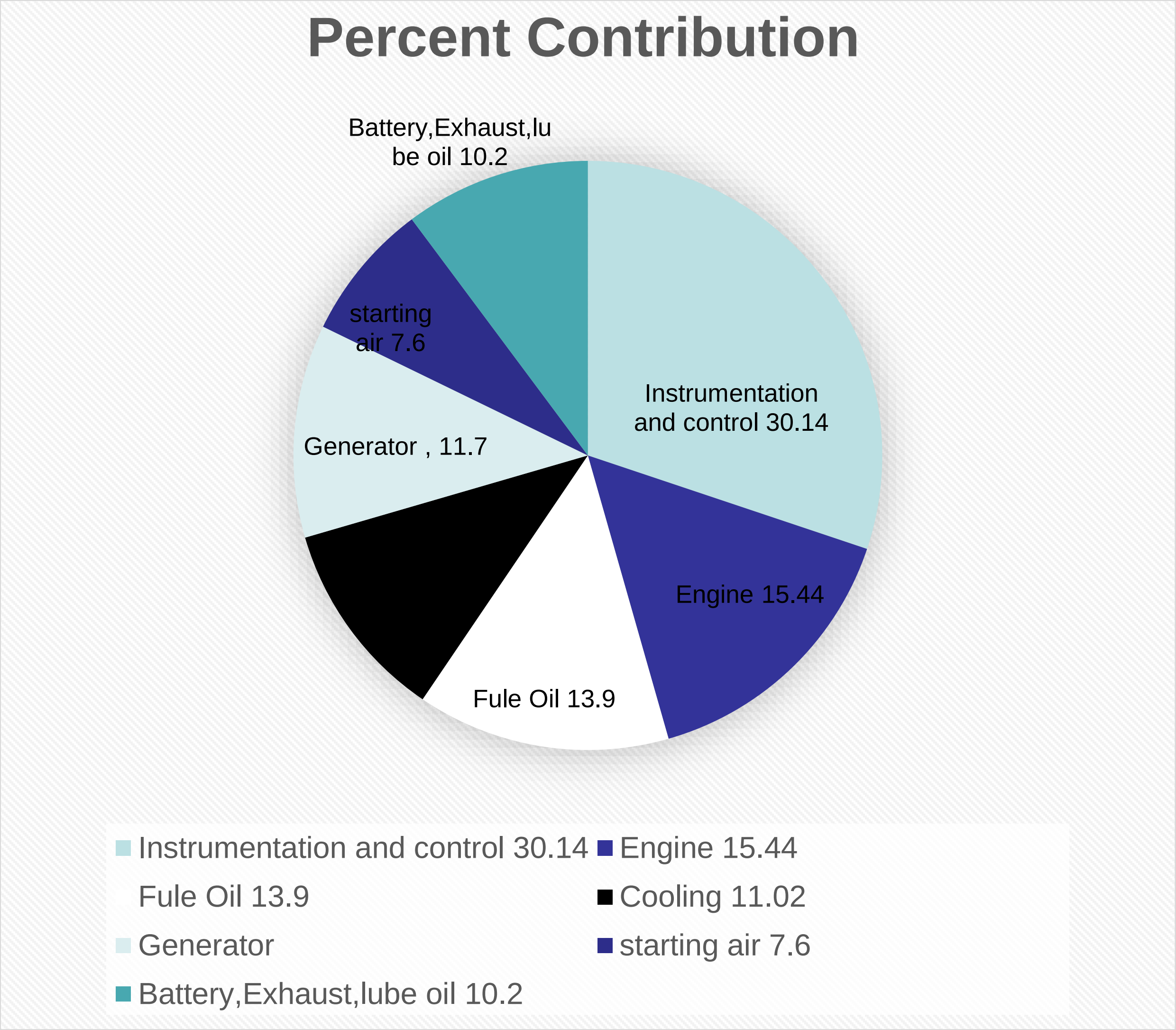
- CCF Root Cause –
  - Design/Construction/Installation/Manufacture Inadequacy and accounted (33%)
  - Internal to Component faults accounted (30%)
  - Human error accounted (22%)
  - To a lesser degree, External Environment and the Other proximate cause categories were assigned to the EDG component.
- CCF Coupling Factor-
  - Design is the leading coupling factor with 66 events (48%).
  - Maintenance with 39 events (28%) accounts for the majority of the remaining events.
  - Environmental ,hardware quality based and operational to the lesser degree.

Ref: NUREG/CR-6819,Vol.1: Common Cause Failure Event Insights

Insights obtained

Review of event Summary of 138 events in the NUREG report led to following conclusions :

- The highest number of events occurred in the instrumentation and control sub-system (41 events or 30%).
- The cooling, engine, fuel oil, and generator sub-systems are also significant contributors. Together, these four subsystems comprise over 50 percent of the EDG CCF events.
- The battery, exhaust, and lubricating oil subsystems are minor contributors.



Review of EDG CCF Events and Identification of vulnerabilities

사단법인 한국원자력학회 KOREAN NUCLEAR SOCIETY

- Instrumentation and Control:
  - Main Failure were in relay and in Governor (approximately 10 each).
  - Failure in governor were also due to relay socket failure or resistor failure due to fatigue.
  - Relay failures were due to dust deposition, incorrect set point or relay socket failure due to high vibration.
- Starting Air System:
  - Most Affected System in compressed air system are valves.
  - Valve failure was due to accelerated aging, Presence of dirt and other contaminations (oil, corrosion products in the starting air system) and procedural error.
- Fuel Oil:
  - Max failures were in Fuel oil pump, pump strainer, Fuel oil tank and leak due to piping, failure of gaskets and O-rings.
  - Failure were due to cavitation of fuel oil pump, wrong valve configuration, high vibrations in piping, fouling of oil and chocking of strainers.
- Cooling:
  - Main Component failed were piping ,valves and Heat Exchanger.
  - Failure were due to corrosion in piping, fouling of cooling water, maintenance error and operational error.

Review of EDG CCF Events and Identification of vulnerabilities

- Breaker:
  - Most contributing component was relay and logic circuit.
  - Failure were due to design error and maintenance error and in some case oxidation /pitting on breaker contact also.
- Engine:
  - Main Failures were in turbocharger, Piston ,shaft .
  - Failures were due to inadequate maintenance ,inadequate lubrication of pistons due to design deficiency, and bad quality.
- Lube Oil:
  - Failure were in Heat exchanger and check valves.
  - Failure were due to design and maintenance deficiency.

Typical Defense against CCF

Defense Strategy for eliminating or reducing the coupling factor

- Diversity: Functional, Equipment, Staff.
- Physical or Functional Barriers: Spatial Separation Physical Protection, Interlocks Removal , or administrative control on cross ties.
- Testing and Maintenance policy: Staggered Testing, Staggered Maintenance.
- Additional Redundancy.

Defense Strategy against causes

- Design Control.
- Use of qualified equipment.
- Testing and preventive maintenance programs.
- Procedure review.
- Personnel Training quality Control.
- Redundancy etc.

CAUSE-DEFENSE MATRIX

Selected Failure Mechanism	Procedural Control/ General Administrative Control			Maintenance/Operational Practices	Design Features
	Configuration Control	Maintenance/Operating Procedure	Test Procedures		
Instrumentation Control Relay Failure due to dust deposition Failure of relay sockets due to high vibration Resistor failure in Governor Governor out of adjustment	-Closure of panel doors where relay are mounted.	-Special Focus on Contact Cleaning in Maintenance Procedure -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 -Improved and Clean Ventilation of relay room -Improved installations of relays
Starting Air System Corrosion products in Air start system Air start Receiver leakage 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 , Monitoring of dew point of dry air, 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 -Material of construction of receiver and piping of air system compatible with air e.g. have SS lining. -Provision of Limit Switch in the valves to get early notification of inadvertent closure.
Cooling: Corrosion in jacket cooling system Improper line up of cooling water system 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. -Proper flushing of sampling bottles before sampling.	-Addition of Corrosion Inhibitors in jacket cooling water system. -Enhanced sampling of Jacket cooling water system. -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 -Design review of Sampling provision to get representative sample.

CAUSE-DEFENSE MATRIX

Selected Failure Mechanism	Procedural Control/ General Administrative Control			Maintenance/Operational Practices	Design Features
	Configuration Control	Maintenance/Operating Procedure	Test Procedures		
Fuel Oil System : Water/sediment/fungus in Oil Fuel Pump strainer blockage Fuel oil Spurious draining/wrong valve configuration Fuel Oil pump priming High Vibration in Piping	-Strict and Improved control of configuration of valves of Fuel Oil System	-Improved maintenance of Pump Suction Strainers. -Self cleaning strainers can be installed.	-Include in TP to measure Vibration of fuel oil system piping during DG running condition	-Regular draining of water and sediments from the tanks -Enhanced Sampling of Fuel Oil. -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 -Incorporation of Syphon in fuel oil suction line to prevent loss of prime. -Venting of Fuel Oil Storage tank with syphon to prevent atmospheric ingress of moisture.
Engine: Turbocharger fan failure due to bad quality 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. -Revisit the design to improve splash lubrication of engine
Lube oil System: Contamination of oil due leak in lube oil cooler 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. -If pressure difference is unavoidable higher pressure should be of lube oil system.

DEFENSE-CAUSE MATRIX

Selected Failure Mechanism	Procedural Control/ General Administrative Control			Maintenance/Operational Practices	Design Features
	Configuration Control	Test Procedures	Maintenance/Operating Procedure		
Breaker: Output breaker failed to close due to oxidation/pitting of contacts Malfunctioning of trip lockout relay 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. -Breaker contacts to be checked during PM for oxidation products.	-Improved ventilation of breaker room

DEFENSE-COUPLING FACTOR MATRIX

Selected failure mechanism	Diversity	Barrier		Testing and maintenance	
	Functional/Equipment/Staff	Spatial Separation	Removal of cross ties	Staggered testing	Staggered Maintenance
Instrumentation Control : Relay Failure due to dust deposition Failure of relay sockets due to high vibration Resistor failure in Governor Governor out of adjustment	-Use of Numerical relays and Electromagnet relay. -Relay Bought from bought vendors	-Spatial Barrier among relays as much as possible	-	-	-
Starting Air System Corrosion products in Air start system Air start Receiver leakage Air Start system valved out	-Compressed Air Dryers working on different principle -Silica Gel Desiccant dryer Membrane Dryer (Nitrogen membranes) -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 . -Additional indication of tie valve position in MCR	-	-Staggered Maintenance of Air receiver tanks and Tie valves
Cooling: Corrosion in jacket cooling system Improper line up of cooling water system Aquatic organism in service water system	-Chemical Addition in Jacket cooling system from different sources may be tried -Diversity in Staff carrying out the Isolation and preparing the permit for isolation. -Checking of DM water quality at two labs.	-	-Removal of cross ties between the make up water to jacket cooling water system	-	-Staggered maintenance of Cooling water system

DEFENSE-COUPLING FACTOR MATRIX

Selected failure mechanism	Diversity	Barrier		Testing and maintenance	
	Functional/Equipment/Staff	Spatial Separation	Removal of cross ties	Staggered testing	Staggered Maintenance
Fuel Oil System : Water/sediment/fungus in Oil Fuel Pump strainer blockage Fuel oil Spurious draining/wrong valve configuration Fuel Oil pump priming High Vibration in Piping	-Staff Diversity in testing and maintenance and sampling 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: Turbocharger fan failure due to bad quality Inadequate lubrication of pistons due to design deficiency	-Diversity in staff for manufacturing ,installation and maintenance.	-	-	-	-Staggered maintenance
Lube oil System: Contamination of oil due leak in lube oil cooler 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: Output breaker failed to close due oxidation/pitting of contacts Malfunctioning of trip lockout relay Out breaker did not closed due to deformed spring retainer	-Diversity in lockout relay can be considered.	-Spatial Barrier among breakers of Different EDGs	-	Staggered testing	-Staggered maintenance

CCF Parameter Estimation

- ***Event Impact Vector-*** For a component group of size m, the impact vector have (m+1) elements. The (k+1)th element, denoted by $F_{k,}$ equals 1 if failure of exactly k components occurred, and 0 otherwise. In case of EDG component group of size 2, possible impact vectors are the following:

  [1,0,0] : No component failed

  [0,1,0]: Only one component failed.

  [0,0,1]: Two components failed due to shared root cause.

- Average Impact vector Ī: To take into account uncertainty in number of component failed due to shared cause.

$$\bar{I} = \sum w_i i_i \quad (i=1 \text{ to } i=N)$$

where, w_i is the weight or probability of hypothesis i with impact vector i_i and N is the Number of Hypothesis.

CCF Parameter Estimation

- Once the impact vectors for all the events in the database are assessed for the system being analyzed the number of events in each impact category by adding the corresponding elements of the impact vectors.

$$n_k = \sum F_k\ (i)$$

where, n_k = total number of basic events involving failure of k similar components

$\sum F_k\ (i)$ = the k-th element of the average impact vector for the event I

- The parameters of the alpha-factor model can be estimated as:

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

where, $\alpha_k^{(m)}$= fraction of the total frequency of failure events that occur in the system involve the failure of k components due to a common cause.

n_j = the sum of the *jth* element of the impact vector, over all events

Estimation of Modified Alpha Parameter for EDG

- With the incorporation of defense discussed, the Generic CCF parameter will no more be applicable Modified CCF Parameter is calculated from Modified Application specific Event impact vector given by:

  $I_r = r * I$

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

- Estimates of r_1 and r_2 is based on the quality of target system defense against the root cause and the coupling factor . NUREG CR/5485 has suggested the following values of r_1 and r_2 :

Strength of defense in comparison with average plant	**Root cause(r_1)**	**Coupling(r_2)**
Complete defense	0.0	0.0
Superior defense	0.1	0.1
Moderately better defense	0.5	0.5
Weaker or no defense	1.0	1.0

- Taking the strength of Defenses proposed as Moderately better defense against root cause and coupling factor Modified Application specific impact vector, is $I_r = 0.25\ I$
- 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 α2 as 0.01175 and α1 as 0.98825.

Conclusion

- Increase of redundancy in DG for the NPPs already having CDF within the range is not advisable as it is not cost effective and hence unjustified.
- The changes proposed in this study are for better defense against cause and coupling factor are in general, part of operation and maintenance programme of NPP and are not an additional cost burden.
- Such enhancement of defence against the CCF will give modest improvement in CDF and reduction in FV value of EDG CCF .
- This approach is specifically helpful in plants that are already under operation and significant modifications are not economically feasible.
- The propose changes to enhance the safety of NPP taking into consideration the practicality of its application.

Thank you for your attention

Questions and comments