Original Article

Preventing cascading failure of electric power protection systems in nuclear power plant

Moustafa Abdelrahman Mohamed Mohamed Moustafa, Choong-koo Chang*

KEPCO International Nuclear Graduate School(KINGS), Department of Nuclear Power Plant Engineering, Republic of Korea

1. Introduction

Cascading failure is the major cause of large blackouts in electrical power systems; this paper analyzes a cascading failure in Hanbit nuclear power plant unit two (2) caused by a circuit breaker (CB) operation failure. This malfunction has been expanded to the loss of offsite power (LOOP). In this study, current practices are reviewed and then the methodologies of how to prevent cascading failures in protection power systems are introduced. An overview on the implementation of IEC61850 GOOSE messaging-based zone selective interlocking (ZSI) scheme as key solution is proposed. In consideration of ZSI blocking time, all influencing factors such as circuit breaker opening time, relay I/O response time and messages travelling time in the communication network should be taken into account. The purpose of this paper is to elaborate on the effect of cascading failure in NPP electrical power protection system and propose preventive actions for this failures. Finally, the expected advantages and challenges are elaborated.

2. Case study of cascading failure in a nuclear power plant

The whole cascading failure event has three phases (starting, expanding and collapsing), and remaining for seconds, minutes or in some cases continuing for hours. A detailed review on power system cascading failures theories, studies and reasons causing power system failures are discussed in Ref. [2,4]. Reference [5] gives detailed review and analysis of the world major cascading failure caused by initiating events and led to system blackouts and the investigation of the main causes of each blackouts such as inadequate planned maintenance work, absence of power system control mechanism, deficiencies with respect to operators, protection and control scheme, protection settings and coordination. This paper, introduces three specific points related to cascading
failure in NPPs, i.e., case study of cascading failure in NPP and their causes, cascading analysis methods, and the importance of emerging technologies which are yet to be implemented in nuclear power plant. In the following paragraphs, there is going to be further explanation about the existing electrical protection system and causes of cascading failure in NPP’s electrical power protection system.

2.1. Initiation of loss of offsite power

On 6th of March, 2018 during normal operation of Hanbit unit two (2) the emergency diesel generator (EDG) was started automatically by the low voltage signal generated from the 4.16 kV medium voltage safety bus. As shown in Fig. 1 the non-safety bus (NB-S02) is supplied with power from the unit auxiliary transformer (UAT#1) and from the start-up transformer (SUT#2) as alternative power source. In the process of replacing the central chiller pump, which is the load of the non-safety bus, the stop signal of the local control panel was initiated to open the central chiller CB so that the operator judged that the central chiller was stopped. In reality, the central chiller circuit breaker was not opened and the central chiller motor pump continued operation, only the central chiller lubrication pump was stopped. As the central chiller pump continued operation with the lubrication function stopped, the bearing temperature rose, resulting in motor winding overheating (phase B) and ground fault (A, C phases) occurred.

2.2. Sequential incident propagation process

In the process of replacement of the central chiller (GB-Z050), one breaker (NB-S02-18) failure was expanded to the loss of offsite power (LOOP). As shown in Fig. 2. ① The CB (NB-S02-18) did not open due to malfunction at the same time, the central chiller pump was still running. Only, the central chiller lubrication oil pump stopped causing the bearing temperature of the chiller to gradually rise (the bearing high temperature alarm was activated) as, the bearing temperature was highly increased thereby resulting in motor winding overheating. In this state, the central chiller instantaneous ground fault relay (50 GS, setting 30A, and operating time 0.1 s) pick-up the fault and activated the CB (NB-S02-18) but the CB wasn’t operated. ② The fault current generated due to motor winding overheating caused the upstream ground fault overcurrent relay (51 N residual type) to trip the CB (NB-S02-01) after specified intentional time delay ③ The operator mistakenly identified that the cause of the failure was cleared and tried switching to the alternate power source from (SUT#2) to restore the loss of voltage by closing CB (NB-S02-03). ④ Due to ground fault in (A, C phases) the ground fault relay of the CB (NB-S02-03) was activated and the CB (NB-S02-03) was tripped. ⑤ The operator attempted to

![Fig. 1. Schematic diagram of event propagation.](image-url)
manually switch to the alternate power source twice to recover the low voltage of the 4.16 kV medium voltage non-safety bus (NB—S02) without the causes of the fault being resolved. After first manual reclosing of the CB (NB—S02-03), the ground overcurrent relay was activated automatically to open the CB (NB—S02-03). In the second reclosing of the CB the ground fault occurred under the same conditions as in the first reclosing of the CB but the CB (NB—S02-03) was not opened. At this time, the ground fault relay of the startup transformer (SUT#2) was activated and the switchyard breakers were opened, also the safety bus (PB—S02) lost power. Subsequently, the low-voltage relay of the safety bus (PB—S02) picked up the voltage loss and the emergency diesel generator (EDG) ‘B’ was automatically started to supply power to the safety bus. So, the failure of the central chiller CB (NB—S02-03) was expanded in a chain leading to loss of offsite power event [4].

2.3. Causes of cascading failure

2.3.1. Causes of unopened central chiller circuit breaker

The 4.16 kV medium voltage non-safety bus experienced low voltage due to the failure of shutting down the central chiller pump during switching operation. It was found that the trip coil of the CB (NB—S02-18) failed to rotate the opening latch due to a stuck open latch roller. The visual inspection of open latch rollers and open latch contacts showed that the surface was not clean. Moreover, poor lubrication of contact surfaces led to a failure of the CB opening. Based on the report result analysis, due to insufficient lubrication for the breaker drive and the possibility of a loss of the lubricant used in the breaker drive, the open rod and the open latch roller contact area were poorly lubricated, which resulted in the failure of the CB open signal.

2.3.2. Causes of switchyard breakers trip

The operator attempted to manually switch to the alternate power source twice by closing the CB (NB—S02-03) to recover the low voltage of the 4.16 kV medium voltage non-safety bus without the fault causes being resolved. Due to the ground fault in (A, C phases) caused by motor winding overheating the ground overcurrent relay (51 N, residual type, 120A, operating time 3 s) pick-up the fault and the CB (NB—S02-03) was tripped, the operator attempted twice manually reclosing the CB (NB—S02-03) to recover the low voltage of the 4.16 kV medium voltage non-safety bus without causes of fault being resolved. In the second attempt of reclosing the CB (NB—S02-03) the ground fault occurred under the same conditions as in the first reclosing of the CB but, the CB (NB—S02-03) wasn’t open due to current transformer (CT) saturation of that CB. The current waveform generated at the time of the first manual closing of the circuit breaker did not show any saturation, but the secondary current waveform was partially crushed and decreased during the second reclosing due to current transformer saturations of the over current protective relay (51 N of the NB—S02-03) CB as shown in Fig. 3 (a, b). At that time, the neutral
overcurrent protection relay of the start-up transformer (51NB, 200A, set value 0.59 s of operation time) pick-up the fault and the switchyard breakers (7F00) and (7F71) were opened, also the safety bus (PB-S02) lost power.

3. Analysis of existing protection and control system

3.1. Electrical protection and control system

Overcurrent protective devices classification characteristics can be either time overcurrent or instantaneous tripping characteristics. So it is logical that for a primary overcurrent protective devices to be backed up by other protective devices which also functioning on overcurrent sensing, but set to operate with more higher levels of time or current. The current protection coordination for the central chiller motor pump is achieved using time over current relay (ANSI device No.51) for incoming feeders, and ground overcurrent relay (50 GS), instantaneous time overcurrent relay (50) and time overcurrent relay (51) for branch feeders. The coordination time interval (CTI) between the downstream and the upstream protection devices has to be considered and followed. According to IEEE, the CTI between downstream and upstream protection devices, should be about 200–250 ms. This CTI cause late trip of the upstream circuit breaker when the circuit breaker of downstream relay fails to trip, this made fault duration getting longer, resulted in bigger damage in the motor winding [6]. Fig. 4 shows the existing ground fault protection relay coordination curve for the central chiller motor pump. The ground fault clearing time by the circuit breaker of the upstream feeder relay in case of failure of the CB of the downstream relay can be calculated as shown in Table 1.

As shown in Fig. 5 when a fault occurs in the motor feeder circuit it would take 191 ms for the CB of the downstream relay (50) and up to 441 ms of the CB of the upstream relay to pick up and clear the fault, that means in case of failure of the upstream CB to clear the fault it continued about 441 ms until the upstream CB pickup and clears the fault, as a result significant thermal energy released causing thermal overheating of the motor stator windings.

![Fault current waveform at first closing](image1)

![Fault current waveform at the secondary reclosing](image2)

Fig. 3. Fault current waveform at first and second closing.
3.2. Prevention of cascading failure and vulnerability of existing system

The main challenge in the existing protection system is the long coordination time interval between the downstream and upstream relay and the lack of communications between the protective devices that results in cascading failure. The existing protection and control system was reviewed and the following countermeasures should be considered to improve design vulnerability of existing system:

- Ensure proper interlocking between the chiller and lubrication pump motor.
- Quicker detection of the temperature rise in the bearing.
- Proposition of new protective methods that has not applied to electric power systems of NPPs yet, in order to reduce delay time between downstream and upstream relay.
- Detection of breaker failure by breaker failure protection relay using emerging technologies.

4. Proposed cascading failure prevention methods

IEC 61850 is a protocol developed for the SAS, but it is also suitable for monitoring and protection for electric power system of nuclear power plants (NPP), because it can exchange information at

Table 1

<table>
<thead>
<tr>
<th>Action</th>
<th>Clearing time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Downstream relay trip time</td>
<td>100 ms</td>
</tr>
<tr>
<td>Lockout relay operation</td>
<td>8 ms</td>
</tr>
<tr>
<td>Five cycle CB</td>
<td>83 ms</td>
</tr>
<tr>
<td>CTI between downstream and upstream relay</td>
<td>250 ms</td>
</tr>
<tr>
<td><strong>Total time</strong></td>
<td><strong>441 ms</strong></td>
</tr>
</tbody>
</table>

Fig. 4. Ground relay coordination curve for central chiller motor pump.
high speed in real time base. In South Korea NPPs, the protection relays have been digitized after Shin-Kori Unit 3-4 (Unit 3 commercial operation starts in Dec. 2016), and existing power plants are also gradually changing to digital relays for future maintenance and management, but IEC 61850 has not been applied yet to electric power systems of NPPs yet. Digitalized monitoring system with IEC 61850 can provide a variety of utility benefits, which includes maintenance predictions, fault prevention, active control, improve commissioning testing, and more accurate end-of-life evaluation. Especially, application of IEC 61850 can involve benefits to NPPs protection coordination; fast fault detection and monitoring; cable quantity reduction, easy use of design change and updates [7]. Among the several benefits of IEC 61850 protection coordination method has been selected to improve current electric power system design in this study. IEC61850 can define the data models by abstracting functions to access this data. This abstraction services prescribed in IEC61850 could be drawn to a variety of communication protocols such as GOOSE (generic object oriented substation event) [8]. One GOOSE message can substitute several wiring enabling functionality between inter devices. The GOOSE messaging allow simple configuration between the protective devices, it can be modified and expanded, when needed, without any added hardware. The IEC61850 based ZSI doesn’t require any extra hardwire connections resulting in material and installation cost saving. Using IEC61850 the communication time between the upstream and the downstream protective devices can be significantly reduced, thereby reducing motor thermal overheating. This kind of communication can be achieved by using any of the following three methods:

- Communication using hardwiring connections between the upstream circuit breakers (NB–S02-01) and the downstream feeder circuit breakers (NB–S02-18).
- Peer to peer communication using serial port channel between the upstream and the downstream protective devices.
- Peer to peer communication using IEC61850 GOOSE message between the upstream and downstream protective devices and through ethernet network.

Peer to peer communication using IEC61850 GOOSE message based ZSI has several advantages than the other two methods because the GOOSE message allows configuration, transmission and reception between the protective devices. It also allowed modification and expansion if needed without any addition of hardware which resulted in reducing equipment cost, reliability enhancement and extensive data recording capabilities [9–11].

4.1. IEC61850 based zone selective method

ZSI is based on currents comparison between protective zones. It has a communication control logic system between downstream and upstream breakers. The IEC61850 GOOSE based ZSI scheme always concern about blocking time. It is used to improve the level of protection in the electrical protection power system, through communication between protective relays across the protected zones to reduce the fault clearing time. During ground fault or phase fault conditions the protective devices electronic interlocking allows the devices close to the fault to override its preset time delay automatically and clear the fault without intentional time delay [10–12]. As illustrated in Fig. 6 when a ground fault occurs at the central chiller motor, both the faulted downstream relay and the upstream relay detect the fault. In order to block tripping the main breaker (NB–S02-01) and avoid loss of power for the whole bus, the faulted downstream relay of the CB (NB–S02-18) sends a blocking signal to block the upstream relay from tripping the upstream main CB (NB–S02-01) thereby averting the whole bus power losses. After fault clearance, fault is not detected any more, but if a fault is not cleared and both the downstream feeder relay and upstream relay still detecting the fault, the main upstream relay will trip the main CB (NB–S02-01) as a backup protection. The result is that other devices remain unaffected by the fault and the fault is cleared more rapidly than the existing protection system without using ZSI. The faster the tripping time the lower the stress energy generated during fault occurrence. The main advantage of applying IEC61850 based ZSI is to reduce blocking time between the downstream and upstream relay to its minimum without affecting relays operations.

During ground fault or phase fault conditions the protective devices electronic interlocking allows the devices close to the fault to override its pre-set time delay automatically and clear the fault without intentional time delay. Accordingly, we need to consider the opening time and communication time between the downstream CB (NB–S02-18) and the upstream CB (NB–S02-01) that requires extended blocking time to give the feeder breakers a time

![Fig. 5. Fault clearing time curve.](image-url)
to operate first and isolate the fault [10]. As shown in Fig. 7. And Table 2. IEC 61850 part 5 defines the GOOSE message transfer time for the trip signal as 10 msec including processing time between downstream and upstream relay, interlocking, inter-tripping and logical discrimination between protective devices.

Several studies reported and tested that GOOSE message transfer time is even less than 10 msec., i.e. 2.5 and 4 msec [13,14]. Depending on network configuration and distance between the relays the overall travelling time between the downstream relay and the main upstream relay would be about 20 ms which includes the generated GOOSE message between downstream (publisher relay) and upstream relay (subscriber relay) when the subscriber relay receives the GOOSE message, it conducts a local logical calculation and sends a confirmation GOOSE message back to the publisher to confirm the fault and subsequently send trip signal to the related CB to trip the fault [15].

So, the fault clearing time between the downstream and upstream relays using IEC 61850 based ZSI can be calculated as shown in Table 3.
The IEC61850 GOOSE based ZSI scheme allows continuous trip signal to the CB but the CB failed to trip within a preset time communication protocol when the protective relay (primary) sent a 4.3. Communication-based breaker failure protection overload relay [16].

Monitoring and a high operation time response of the thermal this fast response time can provide an accurate motor temperature Calculations indicate that the response time of thermocouples in the range of (1msec~e7s ) that will directly influence the operation of thermal overload relay. This paper proposed the use of thermocouples as an adjustable switch instead of RTD for motor protection [17]. So that in case of temperature rise due to loss of lubrication pump the thermocouple can quickly detect the temperature rise before occurrence of ground fault due to insulation failure in the motor winding. A thermocouple is a temperature sensor consisting of two different metals, coupled at one end together for a junction and it is used for motor bearings temperature monitoring in NPPs. The best known and the most used thermocouples is type (K) chromium-nickel aluminum as its temperature curve is virtually linear and its temperature sensitivity does not change during long time. Thermocouples has faster response time than RTDs since they are more likely to be at approximately the same temperature as the area around them [18]. Calculations indicate that the response time of thermocouples in the range of (1msec~0.1 s), compared to RTD response time (1~7 s) this fast response time can provide an accurate motor temperature monitoring and a high operation time response of the thermal overload relay [16].

4.2. Quick detection of temperature rise using thermocouples

Resistance temperature detector (RTD) is used for monitoring motor winding temperature in nuclear power plant [16]. It is used to monitor stator winding of the induction motor by recording possible hot spot or hazard area. Compared to thermocouples, RTDs provides the highest sensitivity but the considerable deficiency of RTD is the cumbersome time of response (1~7 s) that will directly influence the operation of thermal overload relay. This paper proposed the use of thermocouples as an adjustable switch instead of RTD for motor protection [17]. So that in case of temperature rise due to loss of lubrication pump the thermocouple can quickly detect the temperature rise before occurrence of ground fault due to insulation failure in the motor winding. A thermocouple is a temperature sensor consisting of two different metals, coupled at one end together for a junction and it is used for motor bearings temperature monitoring in NPPs. The best known and the most used thermocouples is type (K) chromium-nickel aluminum as its temperature curve is virtually linear and its temperature sensitivity does not change during long time. Thermocouples has faster response time than RTDs since they are more likely to be at approximately the same temperature as the area around them [18]. Calculations indicate that the response time of thermocouples in the range of (1msec~0.1 s), compared to RTD response time (1~7 s) this fast response time can provide an accurate motor temperature monitoring and a high operation time response of the thermal overload relay [16].

4.3. Communication-based breaker failure protection

Breaker failure (BF) protection is used to clear the fault by relay sending trip signals to upstream breakers using the IEC61850 communication protocol when the protective relay (primary) sent a trip signal to the CB but the CB failed to trip within a preset time [19]. The IEC61850 GOOSE based ZSI scheme allows continuous communication between intelligent electronic devices (IEDs), once the overcurrent relay detects a fault, it initiates a direct transfer trip (DTT) signal to the upstream circuit breaker to clear the fault. DTT needs to be dependable during fault conditions to allow the trip signal to be received correctly. This type of peer to peer communications based breaker failure protection can be applied in different ways:

- As a function in IEDs that initiates the breaker failure protection when it receives the trip signal from the relay protecting the faulted power system equipment.
- As a built-in function in the protective IED that detected the fault and issued the trip signal.

Fig. 8 shows the data communication between relays using IEC61850 environment, when a fault occurs in the downstream feeder. The downstream relay IED1 will detect a fault and will issue a tripping GOOSE message to clear the fault. The circuit breaker failure function of CB1 will respond to these GOOSE message and the circuit breaker failure timer will start according to time setting and coordination time interval. When the IED1 initiates a trip signal, it starts a timer and monitoring the CB current, if the current does not go away in a predefined time, the IED1 issues a re-trip or trips the upstream breakers to isolate the faulted one. In case of breaker failure, the breaker failure function will point out this failure and a GOOSE message will be sent over the LAN network to trip upstream breakers and initiate DTT to the upstream relay IED2 to clear the fault. After the downstream relay gets a tripping signal but doesn’t receive tripping signal from the feeder circuit breaker, the downstream relay shall send a breaker failure initiate signal (BFI) through a GOOSE message to the upstream relay to force it to trip the upstream circuit breaker, regardless of whether the blocking time has expired or not. Due to breaker failure importance to the protection system, its testing is very crucial. The test process investigates the pickup value of the current detector and verification of the breaker failure timer that is typically 6~12 cycles, and verifying the reset time of the current detectors [10,12].

5. Results and discussions

This paper proposed practical solutions to prevent cascading failure in NPP’s electric power protection system. Introducing Hanbit NPP as a case study, the three major causes of the failure were defined and the proposed solutions to prevent this failures were described in the above sections and can be summarized as follows:

① when a fault occurs within protective zone the CTI between downstream and upstream relay can be reduced from (250 ms) to (20 ms) using IEC61850 based ZSI with continuous communication between relays as shown in Table 4. If the fault current is detected only in the upstream relay, it means that a fault occurred in the bus or branch circuit breaker, then trip the incoming feeder breaker without time delay. Table 4. Shows the fault clearing time comparison achieved by using IEC61850 based ZSI interlocking compared to existing protection system when fault occurred on the bus or branch breaker.

② Breaker failure (BF) protection is used to clear the fault by relay sending trip signals to upstream breakers using the IEC61850 communication protocol when the protective relay...
Fig. 8. Data communication between relays.

Table 4
Back-up relay fault clearing time comparison.

<table>
<thead>
<tr>
<th>Description</th>
<th>Downstream relay pickup time</th>
<th>Delay time (CTI or Comm.)</th>
<th>Lockout relay</th>
<th>CB opening time</th>
<th>Total clearing time</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Existing protection system</td>
<td>100 ms</td>
<td>250 ms</td>
<td>8 ms</td>
<td>83 ms</td>
<td>441 ms</td>
<td>Hanbit protection system</td>
</tr>
<tr>
<td>Protection system after improvements</td>
<td>100 ms</td>
<td>20 ms</td>
<td>8 ms</td>
<td>83 ms</td>
<td>211 ms</td>
<td>ZSI-IEC61850</td>
</tr>
</tbody>
</table>
(primary) sent a trip signal to the CB but the CB failed to trip within a preset time.
③ Using thermocouples with fast response time can provide a quick detection of motor temperature rise before the failure of the motor insulation and transmit trip signal to CB through digital relay. By using IEC 61850 standard communication protocol and merging unit (MU) the output signal of the thermocouple can be transmitted to digital relay without interference of electrical noise.

6. Conclusion

In nuclear power plants, minor faults often lead to LOOP. This paper proposed measures to detect faults early and prevent spread of accidents, focusing on representative LOOP accidents that actually occurred. The LOOP accident described in this paper as an example was caused by a combination of design logic error, delays in failure detection, poor device performance, and human error. Therefore, each of the causes above was analyzed in this paper. Then, measures such as rapid detection of breaker failure using IEC61850 protocol, rapid detection of motor overheating using thermocouple, and backup for breaker failure detection using BF (breaker failure) relay were proposed. The method presented in this white paper is clear in logic and data, but for the breaker failure relay were proposed. The method presented in this paper as an example was caused by a combination of design logic error, delays in failure detection, poor device performance, and human error. Therefore, each of the causes above was analyzed in this paper. Then, measures such as rapid detection of breaker failure using IEC61850 protocol, rapid detection of motor overheating using thermocouple, and backup for breaker failure detection using BF (breaker failure) relay were proposed. The method presented in this white paper is clear in logic and data, but for the field application requires verification in the test facilities as a future work. The results of this paper can then be applied to all new nuclear power plants, which is expected to greatly contribute to the reliable operation of nuclear power plants.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgement

This research was supported by 2020 Research Fund of the KEPCO International Nuclear Graduate School (KINGS), Ulsan, Republic of Korea.

Appendix A. Supplementary data

Supplementary data to this article can be found online at https://doi.org/10.1016/j.net.2020.06.010.

References