# The Trip Algorithm Design of Plant Protection System in iPOWER

YoungGeul Kim, WoongSeock Choi, JaeHee Yun
*I&C System Engineering Department, KEPCO-E&C, Daejeon, Korea*
*young.g.kim@kepco-enc.com*

## 1. Introduction

Due to the Fukushima accident occurred in March 2011, many countries generating and utilizing nuclear power energy are on the move towards developing countermeasures to deal with similar accident conditions to the Fukushima accident conditions (extended loss of AC power).

One way to prevent fatal disaster outcomes observed from the Fukushima accident is to adopt passive safety systems rather than to keep high dependency on the existing active components in the nuclear power plants (NPPs)[1]. The innovative Passive Optimized World-wide Economical Reactor (iPOWER) has been devised to confirm the feasibility of practically eliminating radioactive material release to the environment in all accident conditions including the Fukushima accident conditions [1].

In this paper, the trip algorithm design of the plant protection system (PPS), one of the crucial safety protection systems, to be applied in iPOWER is introduced and analyzed.

## 2. PPS Trip Algorithm Design

In this section some of the design concepts and techniques used to model the trip initiation algorithm are described. The trip initiation algorithm includes a bistable processing stage, coincidence processing stage, and finally reactor trip initiation processing stage. First of all, the architecture of the PPS in iPOWER is considered in a couple of different aspects.

### *2.1 Architecture*

The PPS in most of the current NPPs consists of bistable processing stage and coincidence stage [2] prior to generating the final reactor trip initiation signal, which is transmitted to the reactor trip switchgear system to open the trip circuit breaker resulting in cutting off the power to the digital rod control system. As for the iPOWER PPS design, a new architecture is considered for application in the main body of the PPS (bistable and coincidence processing stage) in regards to achieving simple design with high reliability/availability effect in general.

Typically, the redundancy within a channel is considered in the safety system design for the two main concerns: increase of plant availability upon single random hardware failure and decrease of system's spurious actuation rate. For the Advanced Power Reactor 1400 (APR1400) instance, there are two bistable processors within one PPS channel performing the same bistable processing logic. This design scheme is to prevent system's spurious actuation upon a single failure that may occur within one bistable processor as well as to keep the plant availability by crediting the safety function of the remaining bistable processor of that channel. However, there are no regulatory requirements for redundancy design within a channel. Also, there are no regulatory requirements for decreasing system's spurious actuation.

In fact, configuring safety system based on four channels already satisfies the single failure criterion since one entire channel can be bypassed for maintenance or testing purposes while another channel is in a failed condition due to a random hardware failure of the safety system component or device.

Especially in the safety system of NPP, simplicity is always preferable and desirable if it satisfies all the regulatory requirements and includes no factors that are likely to degrade the safety function of the system at the same time. Applying additional design concepts or considerations to the minimally-designed simplicity is purely optional and may bring some benefits looking at the bright side. However, the benefits are normally limited to the increase of availability and prevention of system's spurious actuation as described previously. These benefits, in fact, do not seem quite worth the efforts and costs required at the beginning stage of the design.

Considering the simplicity design, the possible architecture of the PPS main body can be seen as shown in Fig.1.

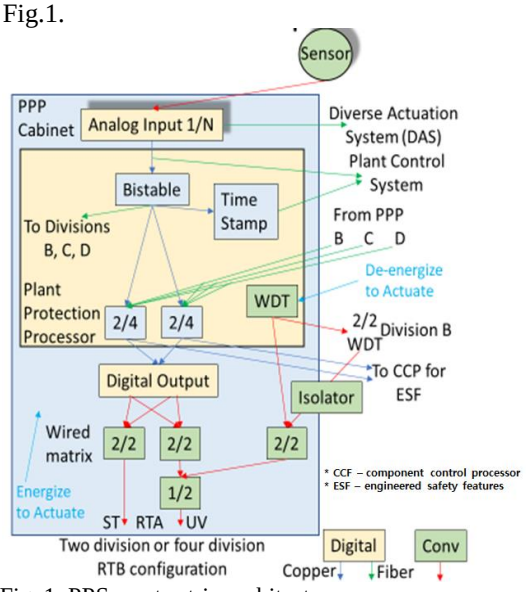


Fig. 1. PPS reactor trip architecture

### *2.2 Software Design*

The configuration of Fig.1 represents one plant protection processor (PPP) that performs one bistable processing logic and two coincidence logics in parallel sequentially. In this configuration just like other types of configuration, all possible cases of spurious actuation of a single safety channel must be considered: a spurious actuation from an erroneous bistable output or from a 2oo4 (two-out-of-four: actuate when there exist two or more valid signals at the same time) voter output itself or processing after 2oo4 voter.

An erroneous bistable output can be prevented by the 2oo4 voter in the PPP. After all, the PPP will provide proper indication relating to the erroneous signal through the self-diagnostics (up to 100% coverage with component-by-component failure modes and effects analysis). An erroneous 2oo4 voter output or an erroneous processing after the 2oo4 voter can be prevented by the PPP self-diagnostics.

It is important to have the self-diagnostic functions be an integral part of the digital platform operating software (OS). As for the self-diagnostic itself, it should be designed to execute deterministically before updating the PPP outputs. Therefore, the PPP holds its last good value upon generating any erroneous output. In case of experiencing fatal errors of the PPP such as memory errors, the PPP shutdown is forced by the self-diagnostics, eventually causing the watchdog timer (WDT) to operate for the targeted fail-safe action. The self-diagnostics are exclusively provided through controller's OS which acquires a safety critical classification. The 100% coverage self-diagnostics are important in that the application software can utilize important diagnostic outputs as far as those outputs play a critical role for application software to take automatic safety actions. Furthermore, those diagnostic outputs can be used to enable the operator to determine what safety-related human actions, if necessary, are required upon any abnormal diagnostic results on top of application software's automatic safety functions.

### *2.3 Design Considerations*

Although the simplicity is preferable and desirable, the following design considerations cannot be neglected when designing the system: fail-safe, fault tolerance, unavailability, spurious actuation of the system, and testability. Essentially, the fail-safe design is achieved from 4-channel basis of the safety system. While one safety channel is in a failed condition due to a random failure, three remaining safety channels still perform their safety functions without being adversely affected by the failed channel.

In other words, the 2oo4 voting functions are automatically converted to 2oo3 voting. Since there are no regulatory requirements for redundancy within a channel, the conversion from 2oo4 to 2oo3 voting due to a random single fault in a channel is tolerated at the system level.

As for the system availability, the following equation is used for the quantitative analysis of the availability of any portion of the system wherever possible:

$$Availability = MTBF/(MTBF + (1-SDC)*T/2+MTTR),$$

where MTBF is mean time between failures (hours), SDC is self-diagnostic coverage (100%), T is periodic manual test surveillance frequency, and *MTTR* is mean time to repair. In the AP1000 design (using two separate bistable processors and one coincidence processor per safety channel), for instance, the availability was calculated to be approximately 0.992986 and this result was based on the early generation digital platform.

Using a modern digital platform for the safety system of iPOWER (using only one PPP for bistable and coincidence processing stage), the newly calculated availability is up to 0.998175. This is because a modern digital platform (safety critical) provides comparatively long *MTBF*, nearly 100% of *SDC*, and short *MTTR*. Especially, it is noted that 100% of *SDC* would make *T* almost meaningless in the availability equation shown above.

When a fatal fault or failure occurs in one channel, the self-diagnostic function will directly and specifically indicate the failure so that the operator can be aware of the problem at once for repair. Furthermore, spurious actuations due to a potential single random failure are analyzed to ensure they are bounded by the design basis events or accidents.

Lastly, the designing the system so that it can be tested during power operation without adversely affecting the safety functions is crucial in obtaining high reliability of the system. In the US-APWR case where no safety-critical grade test processor (typically requiring application level programming to generate and inject functional test signals) is used for testing, the basis for its test method is, surveillance testing taken together with automatic self-testing should provide a mechanism for detecting all detectable failures [3]. This basis does not require that all failures be detected by surveillance testing. Instead, it allows automated self-testing to be credited for failure detection.

Therefore, the innovative design simplicity with high reliability can be achieved through crediting the automatic self-tests and self-diagnostics functions that are built-in to the digital platform OS.

## 3. Conclusions

The PPS trip algorithm that mainly constitutes bistable processing and coincidence processing logic is directly related to the safety function of the protection system in NPPs. For the iPOWER, one possible architecture with simplicity and high reliability design

under various design considerations has been examined for feasibility of the safety protection system.

Implementing one bistable processing logic and two parallel coincidence logics in one processor module rather than using two separate processors can be a good way of achieving innovative simplicity, high reliability, high availability, and enhanced preventability of system's spurious actuation in the iPOWER PPS design as discussed previously. To do so, it is crucially important to apply a modern digital platform adopting a high-speed microprocessor with large memory capacity which is mainly for the application software. By using a modern digital platform, it seems highly feasible to meet the criteria just listed above since it offers relatively long MTBF and relatively short MTTR, which are the major factors affecting the overall system availability.

Likewise, a successful design and implementation of safety-critical grade self-tests that are an integral part of a modern digital platform OS will bring benefits in many aspects such as no need to consider a separate test processor (which will significantly reduce the initial capital cost of the system as well as recurring operation and maintenance costs) and no need for performing manual tests that are usually too time consuming, which, on the one hand, may degrade the system availability.

## REFERENCES

[1] S.W. Lee, S. Heo, H.U. Ha, and H.G. Kim, The Concept of the Innovative Power Reactor, Nuclear Engineering and Technology, Vol.49, Issue 7, p.1431, 2017.
[2] D.Y. Lee, J.G.Choi, and J. Lyou, A Safety Assessment Methodology for a Digital Reactor Protection System, International Journal of Control, Automation, and Systems, Vol. 4, No. 1, pp.105-112, February 2006.
[3] NUREG-0800, Branch Technical Position 7-17, "Guidance on Self-Test and Surveillance Test Provisions", U.S. Nuclear Regulatory Commission, Rev.5, March 2007.