Emerging I&C technologies under the shifting regulatory environment in South Korea

Gyunyoung Heo [1], Poong Hyun Seong [2] and Hyun Gook Kang [2]*

[1] Department of Nuclear Engineering, Kyung Hee University, Youngin-si, South Korea, [2] Department of Nuclear and Quantum Engineering, Korea Advanced Institute of Science and Technology, Daejeon, South Korea

The role of probabilistic safety assessment (PSA) has been supplementary and risk-informed applications based on the insight from PSA have also been utilized limitedly in the licensing process for nuclear power plants (NPPs) in South Korea. However, as the technical significance of PSA is getting increased, PSA has become a mandatory part of Safety Analysis Reports and Periodic Safety Review. It is worthwhile to highlight the role of emerging instrumentation and control (I&C) technologies including human–machine interface (HMI) in developing more credible and realistic PSA models. Particularly, it is expected that the information technology (i.e., software) embedded in digital I&C can adjust over- and under conservatism in analyzing risk. In this study, authors proposed the cases which would be able to significantly reduce risk if advanced I&C supported by information technologies is applied. In regard, the several enabling techniques and their effects are proposed. In order to improve the commercial competitiveness of NPPs, the need of collaboration and synergetic outcome of I&C, HMI, and PSA should be emphasized.

Keywords: nuclear power plant, instrumentation and control, human–machine interface, probabilistic safety assessment, nuclear safety

Introduction

Though there are little differences in the regulatory infrastructures of all nuclear facilities in countries, probabilistic safety assessment (PSA) has performed important roles in optimizing regulatory resources while keeping nuclear safety higher. PSA has been evolved as a decision-making or communicating tool by emphasizing technical vulnerabilities of nuclear power plants (NPPs) since 1970s. Risk-informed applications (RIAs) supported by PSA are particularly useful for allocating limited resource while maintaining as higher standards as practically achievable. The nature of PSA seeks the practical observation for reducing risk, so the PSA model by enabling engineers to find the relative priority of accident scenarios, weak points in achieving accident prevention or mitigation, and insights to improve those vulnerabilities. However, it should be noted that there are still over- and under-conservative aspects in the procedures of developing a PSA model (Heo et al., 2014). The regulatory authority noticed the statement of using PSAs for licensing process of new nuclear reactors in 1989, but after the policy statement, differently from other countries to actively promote the use of PSA, PSA has been supplementary and the RIAs of which the core method is PSA were also carefully and limitedly exploited in the licensing process for NPPs of South Korea. Since 1994, the utility has begun to voluntarily conduct PSAs for operating plants while the legal requirement was not settled down. Recently, the technical position of PSA is being

changed due to the consolidated regulatory needs. PSA has become mandatory section of safety analysis reports (SARs) for construction license and operating permit, and periodic safety review (PSR) performed every 10 years, hence technical responsibility of PSA is getting more important. This should be the results of improved PSA models with less aleatory as well as epistemic uncertainty during the past decades.

Meanwhile, in many countries, the computer-based operator support systems are deployed in NPPs for enhancing both emergency operation capability and broader information support during normal operation. The role and opportunity of instrumentation and control (I&C) including human–machine interface (HMI) should be worthwhile to be highlighted in developing PSA models. Particularly, it is expected that the information technology (i.e., software) embedded in the digitalized I&C systems can adjust over- and under conservatism in analyzing risk due to the increased capability of human performance and the reduction of data variation. The conventional PSA models are not fully and comprehensively dealing with these factors.

In Section "Contribution of I&C in PSA Models," authors analyzed the results of PSA models for OPR-1000 (Korean designed two-loop 1000 MWe pressurized water reactor) and proposed the possible accident scenarios which would be able to significantly reduce risk if advanced information technologies are applied. In order to technically backup these bottlenecks, the enabling techniques such as failure rate uncertainty reduction, component unavailability reduction, and human error (omission and commission) reduction are described in Section "Enabling Techniques," which are representative achievements published by authors' previous researches. Finally, the necessary recommendations and challenges to make synergetic outcome among I&C, HMI, and PSA are discussed in Section "Conclusions and Recommendations."

Contribution of I&C in PSA Models

In this study, authors analyzed the results of PSA models for OPR-1000 and found the accident scenarios which can significantly reduce risk if advanced HMI technologies are applied. In conventional PSAs, which mainly include the models of analog I&C systems, I&C systems were considered as so called support function providers. It means that the function of I&C systems was understood and limited as safety signal generation or processing for supporting front-line systems such as safety valves and pumps. This concept of modeling was valid with simple analog processing circuits of conventional NPPs. The role of I&C systems is changing. As broad and active deployment of digitalized I&C systems is going on, this concept of modeling must be modified since they are becoming an essential part of actual safety operation.

Though digitalized I&C systems were introduced due to the issues of obsolescence, the digital technology seems slowly but successfully matured and smeared into industries. In early 2000, South Korea initiated and finalized a project to localize the major digital I&C hardware through Korea Nuclear I&C System (so called KNICS) Project. Once the digitalized I&C systems are introduced, new technical chances opened by virtue of increased computing capability, huge data warehouse, wide networks, and

so on. This trend ultimately aims at emphasizing the role of I&C, HMI, and operators, which is the critical and never-ending concern on nuclear safety. In conclusion, information technologies can make step forward to enhance operators' and/or maintenance crews' capability.

Meanwhile, the contribution of such digital technologies to the enhanced safety of plants was not considered carefully, or more precisely, their contribution could not be evaluated in a quantitative manner. **Table 1** shows the representative differences between deterministic and probabilistic approaches.

In the deterministic approach, operator's response is assumed to be a certain fixed pattern. Therefore, there is no method for augmented operator's capability to be reflected. Even though human error probability is considered in the probabilistic approach, the operator's behavior in digitalized environment is not fully understood; so, we are not able to make sure whether the current PSA model over- or under-estimates results. As an example, feed & bleed operation in a PWR is the last mean of removing residual heat from the core and its failure probability caused by human error is around 23% because of short time, high stress level, and consequence significant decision. Another critical safety operation, aggressive cool down, was also reported to have very high failure probability (Jung et al., 2007). In a modern digital control room, the human operator actions could not be decoupled from the digital support systems which provide required processed information in a timely manner and support execution of actions with computerized procedures. Enhanced information system and support system would reduce the failure probability of some safety-critical operations.

More aggressive utilization for risk reduction of NPPs comes from online testing or monitoring of frontline safety components. Automatic online monitoring and testing assures the success of component actuation when its demand comes. The failure

TABLE 1 | Comparison between deterministic and probabilistic approaches.

	Deterministic approach	Probabilistic approach
Initiating events	Limited to design basis accidents (some beyond design basis accidents may be included)	All potentially important events are included
Equipment reliability	Single failure criterion is postulated	Multiple failures and common cause failures are also considered
Operator behavior	For $t < T$, no action is postulated ($T = 10 \sim 30$ min) For $t > T$, no operator errors are postulated	Errors in diagnosis and execution are considered throughout the accident sequence
Analysis	Conservative assumptions; orbest estimate + uncertainty	As realistic as possible
Use of results	Comparison with absolute acceptance criteria	Assess the safety in relative manner -Important accident sequence -Weak points in design and procedures

probability of a component which was tested 1 s ago is much lower than that was tested 1 month ago. Furthermore, this automatic testing and monitoring technology provides much higher chance of alternative operation path selection by operators to avoid the use of failed components.

Intelligent operation procedure can be achieved by integrating information and digital MHI technologies. Conventional operation procedures were developed in consideration of balancing between the efficiency and simplicity under analog signal processing circumstance. Technical support for safe operation from various intelligent agents in modern NPPs could change the emergency operation procedure itself.

Enabling Techniques

According to the aforementioned chapter, it is expected that controlling risk can be managed in a better manner when advanced information technologies are adopted. This chapter describes such enabling techniques to support the technical gaps identified in the PSA model.
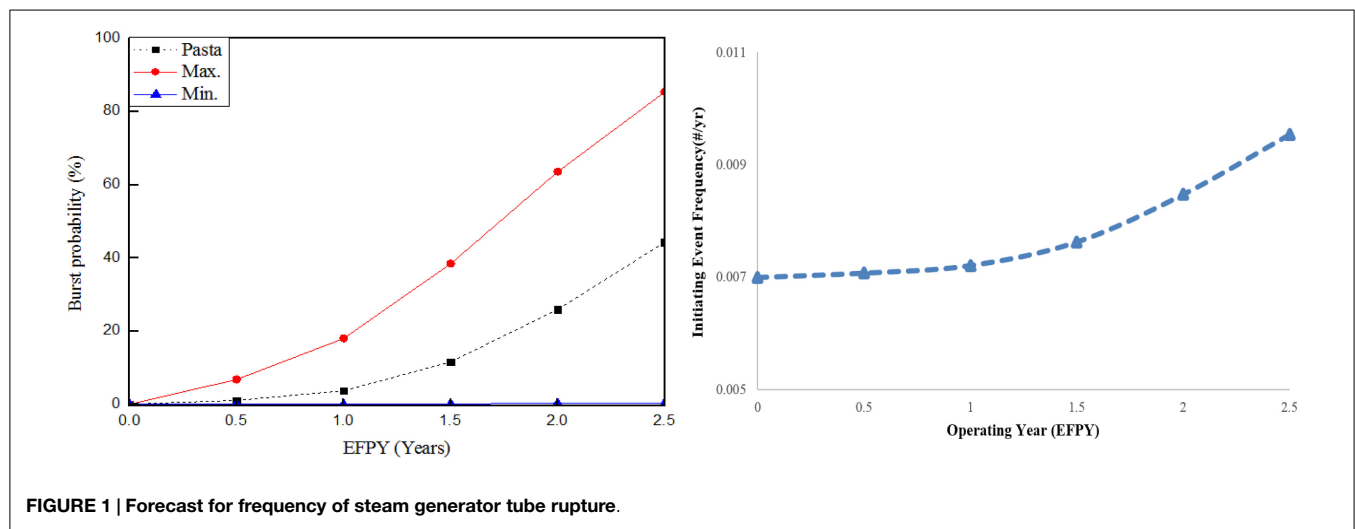
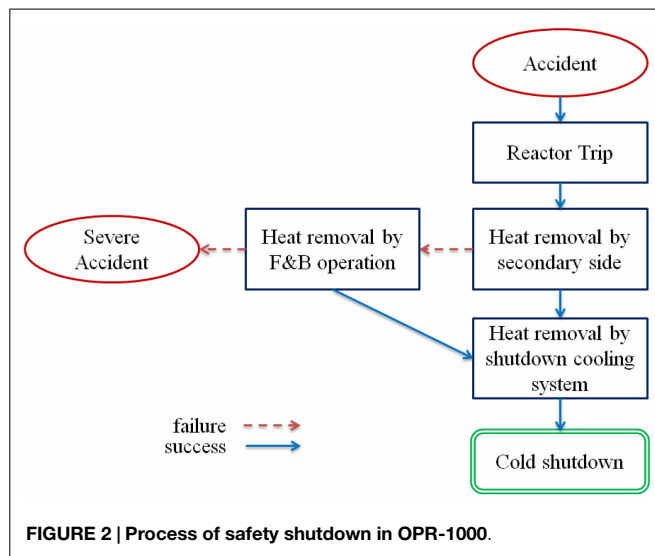### Update of Initiating Event Frequency upon Conditions

The initiating event (IE) frequency currently used in a PSA model is a kind of averaged and lumped result during the whole plant life-time. This idea came from the reliability theory. The well-known bathtub curve representing component's failure rate is divided into three parts: infant failure, random failure, ware-out failure. In order to avoid stochastic failures during the beginning and the end periods, NPPs make trial runs and make use of the preventive maintenance strategy. The failure rate of the component in NPPs is, therefore, subjective to constant and random pattern in the bathtub curves. However, a digital technology can clarify two significant phenomena: one is the fluctuation of failure rate even though it was assumed to be constant, and the other is to detect the point of departure to wear-out failure interval. Under the digitalized environment, the condition monitoring and prognostic can track the trajectory of the failure rate even in the constant and random failure rate interval. While there should be

benefits in using information technologies, its uncertainty must be a concern from the viewpoint of regulation. In regards, US Nuclear Regulatory Commission (NRC) concluded 14 technical issues should be resolved for allowing the acceptance criteria (Hines et al., 2008). Currently, condition monitoring and prognostic is not generally accepted by regulatory authorities, it needs to be noted that there was the case that a surveillance technique had been officially approved for the helicopter rotor (Sikorsky Aircraft Corp, 2015).

In fact, the IE frequency is obviously changing upon degradation and operational conditions. As the inspection and prognostic techniques are getting advanced, it becomes possible to monitor and forecast the detailed and accurate degradation status for significant structures, systems, and components (SSCs). This can properly update the IE frequencies to estimate actual core damage frequency (CDF) representing the state of plant in time-dependent manner.

To provide a case study, authors attempted to analyze a steam generator tube rupture (SGTR) accident (Heo et al., 2014). Since SGTR is a frequent and serious accident; the cracks in the tubes are periodically detected and their growth rate is conservatively estimated by physical or empirical models. It should be noted that this procedure is a part of aging management, but not an input for updating PSA models. On the other hand, NUREG/CR-5750 (Poloski et al., 1998) provides the method to estimate the IE frequency for SGTR. This frequency keeps constant during the whole plant lifetime but can be regarded as a prior distribution for Bayesian update. For instance, in the case of SGTR, the actual incident resulting from stress corrosion cracking (SCC) and wear damage was frequently reported in domestic and foreign papers. For this reason, the structural and burst integrities of SG tubes in static and transient conditions are required to be secured due to the potential for radioactive contamination to the secondary system caused by above damage modes (Kim et al., 2012a). For an illustrative purpose, this study conducted time-dependent probabilistic assessment for the outside axial crack using Probabilistic Algorithm for Steam generator Tube Assessment (PASTA) program (Kim et al., 2012b). The left side of **Figure 1** shows an example of burst probability with effective full power year

FIGURE 1 | Forecast for frequency of steam generator tube rupture.

FIGURE 2 | Process of safety shutdown in OPR-1000.

(EFPY) with uncertainty bands for taking exploratory variables' randomness.

In order to update the prior probability by this prognostic result, we need to develop a likelihood function and Bayesian update so that finally posterior probability for the IE can be calculated, as shown on right side of **Figure 1**. It can be concluded that this approach will reduce the uncertainty in estimating the IE frequency in terms of reactor operating time, making the aging based prediction of time-dependent CDF possible.

Automation of Safety Functions

The operator of a NPP must handle a large number of dynamic information sources and reach a decision to achieve a system goal efficiently and safely. Automation is one of the best ways which reduce operator's workload in main control room (MCR). The automation must be implemented in a balanced manner with manual safety actions for achieving minimum risk.

OPR-1000 has feed-and-bleed (F&B) operation procedure to cope with an accident of which condition limits the cooling capability through steam generator. The F&B operation is the process to remove the decay heat by evaporation of injected water. If adequate heat removal capability through the steam generators is not available, heat can be removed from the reactor coolant system (RCS) by the F&B operation as shown in **Figure 2**. In an OPR-1000, the F&B operation consists of the use of a safety depressurization system (SDS) and safety injection system (SIS). For the F&B operation, operators must manually open the SDS valves, and a safety injection actuation signal (SIAS) should be generated to force the high-pressure safety injection (HPSI) pumps to inject coolant into the RCS. The F&B operation includes a number of steps following the opening of the SDS valves before reaching a shutdown cooling system (SCS) (Kim et al., 2014).

In order to initiate the F&B, the operators need to know the plant status clearly and to have confidence that this operation would be successful. This process takes considerable amount of time, thus operator's failure probability would be relatively high. Operators may hesitate to initiate the F&B operation unless a clear cue is provided because its initiation will result in the release

of radioactive coolant into containment structure. According to safety analysis, operators have to initiate the F&B operation no later than 23 min after a reactor trip to prevent core damage (Jung et al., 2007). Operators also consider the economic losses before the initiation of F&B operation, because it would cause the contamination of in-containment structure and components. Moreover, operators have little experience to perform the F&B operation. Automation of this process is expected to help operator's F&B operation initiation.

While automation is apparently able to reduce human errors so that it can make the CDF decreased, there are still challenges: Enough process parameters must be measured, but a number of parameters, such as the peak cladding temperature, are difficult to be observed due to the absence of direct instrumentation. To apply this strategy to actual plant operation, the method for connection between automation and I&C systems should be developed. To initiate the F&B operation, the automation gathers the signals and generates the actuation signal for safety system from I&C system. Operation strategy for automation should be applied to conventional operation procedure properly and the PSA model needs to be developed for estimating the effect of application of automation. Furthermore, its liability when automation is failed seems very critical to make this concept practically forward.

Component Unavailability Reduction through Monitoring

There are many safety standby systems to mitigate consequences of an accident in NPPs. The entire reliability of safety standby systems greatly depends on the successful operation of some standby component which is supposed to move mechanically (Buchner and Fabian, 1994). Standby equipment does not provide any information for the perception of equipment condition because it is not in operation. Currently, periodic testing is performed to check its abnormalities (Čepin and Mavko, 1997). However, frequent testing can cause the increase of component unavailability by leading aging effect. The maintenance bypass process also makes component partially unavailable. It is desirable that some monitoring techniques be applied to monitor abnormalities of standby equipment without actual operation of component. When a failed state is verified through the monitoring technique, it can be maintained directly; thus, unavailable time caused by a failed but overlooked state can be removed. **Figure 3** shows the monitoring concept for component unavailability reduction. The monitoring method itself does not improve the actual equipment availability but it makes immediate repair possible to be conducted. When the immediate repair is assumed, the unavailable time caused by a failed but overlooked state can be removed.

To set the practical method, first of all, important components should be identified and their dominant failure modes should be determined. Then the signal accuracy and the logic for failure judgment should be considered when an actual sensing technique is applied. Two problems may arise in terms of signal accuracy and failure judgment. When a sensing device cannot detect failures or a failure is ignored, it is the same case the component is not monitored. Alternatively, when a sensing device generates the wrong

FIGURE 3 | Component unavailability reduction through monitoring.
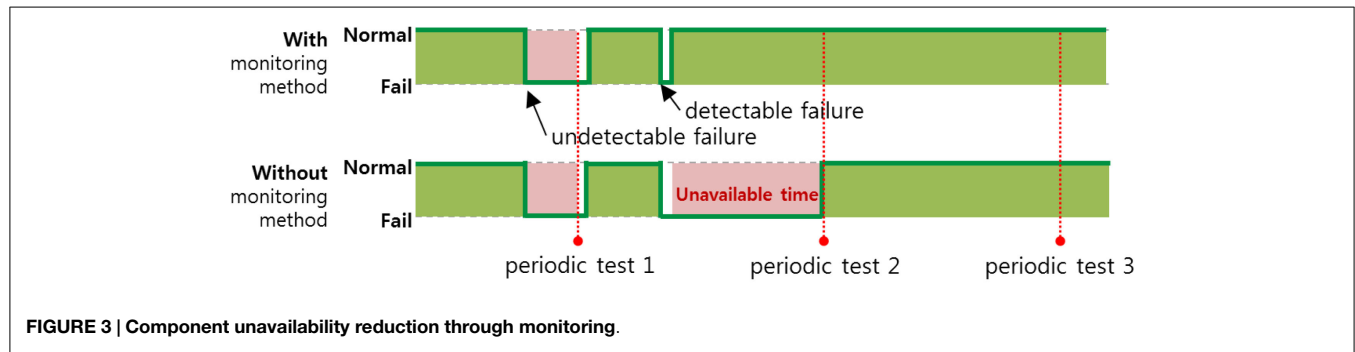
alarm, confusion and unnecessary testing will occur resulting in increase of component unavailability. Therefore, accurate failure detection is one of the key challenges for monitoring of safety critical standby component.

On-line monitoring for standby systems can be equivalently considered as the super-frequently periodic tests, so this technique can greatly reduce the unavailability between testing intervals in the basic events.

State-of-the-art Techniques for Substantial Reduction of Human Errors

In NPPs, the systems are controlled by human operators and I&C systems provide a major source of information to MCR operators (Kim and Seong, 2006). In this environment, the errors caused by human operators can lead unwanted problems. It was found that human error probability has about 62% contribution to CDF (Gertman et al., 2002). Among the solutions to reduce human errors, a new framework for human reliability analysis (HRA) method to predict human error probabilities (HEPs) to provide HEP to PSA is addressed in detail as follows.

The operation environment of MCRs in NPPs has changed with the adoption of new human–system interfaces that are based on computer-based technologies. Among the many features of advanced MCRs, soft controls are the particularly important feature because of the operation actions in NPP. In order to develop the framework for the HRA method in soft control environment, task analysis should be performed to identify human error modes. Moreover, dependency among subtasks is considered by modifying the determination of levels of dependency in the Technique for Human Error Rate Prediction (THERP) model. In the proposed model, a success path is considered to calculate soft control execution HEP with consideration of dependency between two subtasks. A database for inputs to the general HEP equation, such as nominal HEPs and recovery failure probabilities, is developed and applied to estimate HEPs (Jang et al., 2014).

Many statistical results from safety reports tell that training operators for the technical and non-technical skills can prevent many types of human errors. In author's previous study, an effective training of operation teams in the form of integrated model of technical and non-technical skills was suggested. Technical skills were indirectly measured by situation awareness (SA) which was closely related to the level of knowledge. SA was structured by production rules (WHEN-THEN logic) and quantified by Bayesian inference. Four non-technical skills were summarized

and selected from researches of other safety critical industries: leadership, communication, SA, and decision making skills. The selected skills were quantified based on the representative factors (Yim et al., 2013).

Evaluation on Human Error Impact during Test/Maintenance

While automation is the aid for operators, proactive simulation technique can be the aid for test/maintenance crews in NPPs. It is also possible to reduce human errors related with not only operation but also test/maintenance using information technology. Simulation techniques help maintenance crews to recognize which task is the most critical in increasing CDF before they perform their missions.

The framework, shown in **Figure 4**, was proposed for estimation of qualitative and quantitative consequences of human errors that occur during maintenance tasks (Heo and Park, 2010). One of the remedies for unexpected reactor shutdowns may be a systematic tool designed to warn potential hazards arising from a given maintenance tasks, taking into account human error modes in a proactive manner, in terms of risk and/or loss of electrical power. The entire framework that we established is composed of four components: (1) the human-error analyzer to connect possible failure modes resulting from human errors with other estimators, (2) the frequency estimator to quantify the occurrence of maintenance-related failure modes, (3) the risk estimator to determine minimal cutsets and to compute the variation of the CDF using the fault tree analysis and turbine cycle simulation, and (4) the derate estimator to determine the electrical power loss under abnormal plant configurations caused by human error. The final result is characterized by a cost metric that can be used for decision-making possibly resulting in revisions of procedures or task modifications. This idea is more useful for test/maintenance than operation because the simulation technique can be fully used with enough time, which is not practical in emergency operational scenarios.

The conventional PSA models include limited number of human errors during test/maintenance. This method can reduce the uncertainty in PSA model and enhance its use from a different perspective. It provides an efficient mean to address the effect of test/maintenance human errors in a systematic way. Analysis of human errors during test/maintenance with aid of simulation technique can contribute to the reduction of such errors and result in enhanced plant safety.
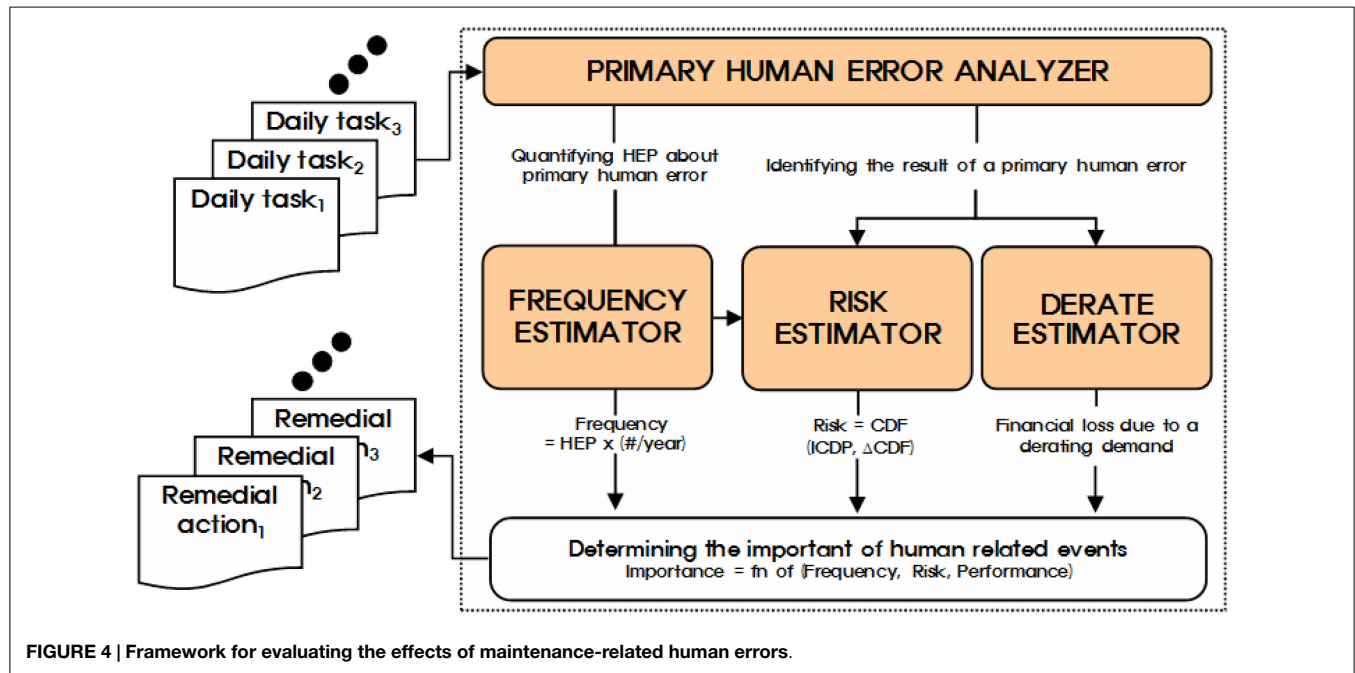
FIGURE 4 | Framework for evaluating the effects of maintenance-related human errors.

Conclusions and Recommendations

This paper emphasizes on the contribution of I&C or information technologies beyond the conventional I&C systems in the field of nuclear safety. Particularly, the digitalized systems are being introduced to recent NPPs and advanced information technologies are expected to take high responsibility of safety and performing desire functions with high reliability. However, to gain confidence, risk contribution of such technologies should be quantified and fully counted with respect to nuclear safety.

Recently, the new policy statement for PSA and RIA has been announced in South Korea, and this should act as a driving-force of the new and emerging HMI researches. In order to keep the strong motivation and feasibility of such approaches, the methods to make up weakness as well as to boost strength

should be supported. From this viewpoint, the benefit of advanced HMI technology can be explained by the reduction of risk in a PSA model. However, there are still lots of challenges: software reliability, quality and quantity of sensing elements, viable monitoring techniques, and inherent uncertainty in statistical approaches and the likewise. These issues should also be resolved to promote the use of advanced HMI technologies in future NPPs.

In South Korea, major digital I&C hardware were successfully developed through KNICS Project, started in early 2000. Now it is time to step forward in software R&D to make synergetic outcomes such that it can be integrated with the digital I&C hardware. Authors expect that this paper would help the researchers and R&D policy managers to recognize issues for promoting safer nuclear energy.

References

Buchner, H., and Fabian, H. (1994). Comparative evaluation of active vs passive system designs. *Reliab. Eng. Syst. Saf.* 45, 195–200. doi:10.1016/0951-8320(94)90085-X

Čepin, M., and Mavko, B. (1997). B. "probabilistic safety assessment improves surveillance requirements in technical specifications,". *Reliab. Eng. Syst. Saf.* 77, 56–69.

Gertman, D. I., Halbert, B. P., and Parrish, M. W. (2002). *Review of Findings For Human Performance Contribution to Risk in Operating Events*. Washington, DC: U.S. NRC. NUREG/CR-6753.

Heo, G., Chang, Y. S., and Kim, H. (2014). "Improvement of PSA models using monitoring and prognostics," in *International Symposium on Future I&C for Nuclear Power Plants/International Symposium on Symbiotic Nuclear Power Systems 2014*, (Jeju).

Heo, G., and Park, J. (2010). A framework for evaluating the effects of maintenance-related human errors in nuclear power plants. *Reliab. Eng. Syst. Saf.* 95, 797–805. doi:10.1016/j.ress.2010.03.001

Hines, J. W., Garvey, D., Seibert, R., and Usynin, A. (2008). *Technical Review of On-line Monitoring Techniques for Performance Assessment*. Washington DC: U.S. Nuclear Regulatory Commission. NUREG/CR-6895.

Jang, I. S., Kim, A. R., Jung, W. D., and Seong, P. H. (2014). An empirical study on the human error recovery failure probability when using soft controls in NPP advanced MCRs. *Ann. Nucl. Energy* 73, 373–381. doi:10.1016/j.anucene.2014.07.004

Jung, W., Park, J., Kim, J., and Ha, J. (2007). Analysis of an operators' performance time and its application to a human reliability analysis in nuclear power plants. *IEEE Trans. Nucl. Sci.* 54, 1801–1811. doi:10.1109/TNS.2007.905163

Kim, B. G., Yoon, H. J., Kim, S. H., and Kang, H. G. (2014). Dynamic sequence analysis for feed-and-bleed operation in an OPR1000. *Ann. Nucl. Energy* 71, 361–375. doi:10.1016/j.anucene.2014.04.014

Kim, H. S., Shim, H. J., Oh, C. K., Jung, S. G., Chang, Y. S., Kim, H. D., et al. (2012a). "Development of probabilistic program for structural integrity assessment of steam generator tubes," in *The Korean Society of Mechanical Engineers Fall Annual Conference*, Changwon, Korea. 477–481.

Kim, H. D., Kang, Y. S., Jo, N. C., Lee, K. H., Jung, S. G., Kim, H. S., et al. (2012b). *Development of Probabilistic Integrity Evaluation Method for Steam Generator Tube Considering Multiple Variables*. Daejeon: Korea Hydro & Nuclear Power.

Kim, M. C., and Seong, P. H. (2006). A computational method for probabilistic safety assessment of I&C systems and human operators in nuclear power plants. *Reliab. Eng. Syst. Saf.* 91, 580–593. doi:10.1016/j.ress.2005.04.006

Poloski, J. P., Marksberry, D. G., Atwood, C. L., and Galyean, W. J. (1998). *Rates of Initiating Events at U.S. Nuclear Power Plants: 1987-1995*. Washington, DC: U.S. NRC. NUREG/CR-5750.

Sikorsky Aircraft Corp. (2015). *HeliHub*. Available at: http://helihub.com/2012/11/08/sikorsky-uses-hums-data-to-extend-life-of-s-92-main-hub/

Yim, H. B., Kim, A. R., and Seong, P. H. (2013). Development of a quantitative evaluation method for non-technical skills preparedness of operation teams in nuclear power plants to deal with emergency conditions. *Nucl. Eng. Des.* 255, 212–225. doi:10.1016/j.nucengdes.2012.09.027

Conflict of Interest Statement: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.