Applications of PSA in Human Factor Engineering Design and Design Reliability Assurance Program for CAP1000

Qiu Yongping, He Jiandong, Zhuo Yucheng
(Shanghai Nuclear Engineering Research and Design Institute, Shanghai, China)

Abstract: PSA plays an important role in reducing the risk and improving the safety and economy of nuclear power plants (NPP). PSA applications are becoming more and more important and extensive. The applications of PSA in Human Factor Engineering (HFE) Design and Design Reliability Assurance Program (D-RAP) for NPP are discussed in this paper. First, a brief description of the methodology is presented. Second, based on a plant-specific PSA model, the application examples are given. The critical human actions and risk-important tasks are identified with some relevant criteria and addressed in HFE design activities to improve the design of human-system interface, procedures and training program. Thus, the likelihood of personnel errors could be minimized and measures for error detection and recovery could be provided. In the application of PSA for D-RAP, the risk-significant structures, systems and components (SSC) are identified based on the importance measures in PSA results and are included in D-RAP management.

1. Introduction
Human Factors Engineering (HFE) for Nuclear Power Plant (NPP) is a complex systematic engineering of Human-System Interface (HSI), and it is helpful for NPP designers to perform design tasks more reliably and configure resources and environment for tasks performance more reasonably. Human Reliability Analysis (HRA) is an integral activity of a complete probabilistic safety assessment (PSA), and seeks to evaluate the potential for, and mechanisms of, human error that may affect plant safety. Thus, HRA is an essential element in achieving the HFE design goal of providing a design that will minimize personnel errors, allow their detection, and provide recovery capability. The Design Reliability Assurance Program (D-RAP) is implemented as an integral part of the plant design process to provide confidence that reliability is designed into the plant and that the important reliability assumptions made as part of the PSA, will remain valid throughout plant life.
In this paper, the methodology of PSA applications in HFE Design and D-RAP is briefly described first. Then, based on the CAP1000 (Chinese Inland Project of AP1000 Standardization Design) PSA model, the risk-significant human actions and SSCs are selected and some examples are presented. Finally, the results are discussed and some conclusions are obtained.

2. Methodology of Integration of HRA with HFE Design
There are certain interfaces between HRA and other HFE elements such as task analysis, procedure development, human system interface design, staffing, training program development and human factors verification and validation. Figure 2-1 illustrates the relationship between the HRA and the rest of the HFE program.\[1\][2]

HRA are conducted early in the design process, so it is necessary to make assumptions about functional allocation, human actions performance, and the quality of the HSI design, procedure, and related performance shaping factors, which should be confirmed and refined as the design effort progresses.

HRA provides inputs and important design insights for functional requirement analysis and allocation, task analysis, procedure development, HSI design, staffing, and training program development.

The critical human actions in HRA of HFE are defined with two alternative criteria:
Deterministic criteria: Any human action that is required to prevent core damage or severe release in licensing design basis accidents, or

PSA criteria: Any human action (as identified from those baseline PSA studies with quantitative results) that, if failed, would result in total core damage frequency (CDF), or large release frequency (LRF), equal to or greater than a certain value. Generally, the threshold value for screening of critical human actions could be set as 1E-4/yr for CDF and 1E-5/yr for LRF.

Qualitative and quantitative criteria are used to screen the risk-important tasks. Risk-important tasks that involve human actions will be identified using two risk-important measures, i.e., Risk Achievement Worth (RAW) and Risk Reduction Worth (RRW). RAW examines the increase in risk that would result if the human error for the task were set to 1.0. RRW examines the decrease in risk that would result in if the human error for the task is set to 0.0.

The analysis is performed based on the results from both the baseline PSA study and the focused PSA study. A focused PSA study is performed to provide input to regulatory treatment of non-safety-related systems. In this case, no credit is taken for non-safety systems in the calculation of core damage frequencies (CDFs) and large release frequencies (LRFs).

A task will be defined as risk important if its RAW or RRW is greater than the risk threshold. For qualitative criteria, the results of quantitative criteria integrated with some other consideration will be used to identify the risk-important tasks by expert panel.

3. Methodology of PSA Application in D-RAP

The D-RAP includes a design evaluation of the plant and, from plant design perspective, identifies the aspects of plant operation, maintenance, and performance monitoring pertinent to risk-significant SSCs. In addition to the PSA, deterministic tools, industry sources, and expert opinions are used to identify and prioritize those risk-significant SSCs.

The initial task of the D-RAP is to identify risk-significant SSCs to be included within the scope of the program. The plant PSA, together with the expert panel, is used to identify those SSCs, consistent with the criteria for Risk Achievement Worth (RAW), Risk Reduction Worth (RRW), and Fussel-Vesely Worth (FVW). A component’s RAW is the factor by which the plant’s core damage frequency increases if the component reliability is assigned the value 0.0. A component’s RRW is the amount by which the plant’s core damage frequency decreases if the component’s reliability is assigned to 1.0. FVW is a measure of an event’s contribution to the overall plant core damage frequency.

Deterministic considerations are also important in identifying risk-significant SSCs. The deterministic identification of risk-significant SSCs includes several guidelines and considerations. In addition, risk-significant SSCs are selected using industry experience, regulations, and engineering judgment.

Scoping of SSCs and reliability assurance development, as well as incorporating this information in design, procurement, construction, maintenance, and operation documentation is a living process. The D-RAP continuously monitors design changes and plant-specific features.

Suppliers of D-RAP SSCs are required to supply an operating experience report in order to provide reasonable assurance that the D-RAP reliability is maintained. Quality assurance and
control during the design, fabrication, construction and pre-operation testing for SSCs scoped in D-RAP is implemented using relevant Quality Assurance (QA) programs.

4. Integration of HRA with HFE Design for CAP1000

The PSA model for CAP1000 is used in this analysis. This PSA model includes internal and external events for level 1 and 2 under different operation conditions. Considering the low plant baseline CDF, a CDF of 1E-5/yr is conservatively defined as the threshold value for screening of critical human actions. However, no critical human action is obtained. The risk-important human error events are screened with the following threshold values based on the baseline PSA results:

- RAW value of 3 or greater, or
- RRW of about 1.1.

For the focused PSA study, a RAW of 2.0 or a RRW of 1.05 is used as the cutoff values. Totally about 20 risk-important human actions are obtained. Some examples are given in Table 4-1. The risk-important human actions are then used as inputs to the task analyses performed as part of the HFE program.

Table 4-1 Examples of Risk Important Human Actions

<table>
<thead>
<tr>
<th>Basic Event ID</th>
<th>Basic Event Description</th>
<th>Screening Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIB-MAN00</td>
<td>Failure to diagnose a SGTR</td>
<td>RAW&gt;3.0 (for CDF and LRF) with baseline PSA model</td>
</tr>
<tr>
<td>CIB-MAN01</td>
<td>Failure to close main steam isolation valve to isolate the faulted SG, given a SGTR</td>
<td>RAW&gt;3.0 (for CDF and LRF) with baseline PSA model</td>
</tr>
<tr>
<td>LPM-MAN02</td>
<td>Failure to recognize the need for RCS depressurization during a medium LOCA</td>
<td>RRW&gt;1.1 (for CDF and LRF) with baseline PSA model</td>
</tr>
<tr>
<td>ATW-MAN03</td>
<td>Failure to recognize and manually trip the reactor (through PMS) in one minute</td>
<td>RAW&gt;2.0 and RRW&gt;1.05 (for CDF and LRF) with focused PSA model</td>
</tr>
</tbody>
</table>

5. Design Reliability Assurance Program for CAP1000

CAP1000 PSA model is used in this analysis. The following components are considered for inclusion in the D-RAP:

- RAW values of 2 or greater,
- RRW of 1.005 or greater, or
- Fussel-Vesely worth of 0.5 percent or greater.

Totally about 20 systems are included with the relevant components in the list of SSCs for D-RAP. Some examples are shown in Table 5-1. It should be pointed out that expert judgement is also very important for the analysis of SSCs included in D-RAP.
Table 5-1  Examples of Risk-Significant SSCs within the Scope of D-RAP

<table>
<thead>
<tr>
<th>System, Structure, or Component (SSC)</th>
<th>Rationale$^{(i)}$</th>
<th>Insights and Assumptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>System:  Class 1E DC Power and UPS (IDS)</td>
<td>RAW/CCF</td>
<td>The batteries provide power for the PMS and safety-related valves. The chargers are the preferred source of power for Class 1E dc loads and are the source of charging for the batteries. The inverters provide uninterruptible ac power to I&amp;C system.</td>
</tr>
<tr>
<td>250 V dc 24-hour Buses, Batteries, Inverters, and Chargers</td>
<td>RAW/CCF</td>
<td></td>
</tr>
<tr>
<td>System:  Protection and Safety Monitoring System (PMS)</td>
<td>RAW/CCF</td>
<td>The PMS software/hardware provides the automatic reactor trip and ESF actuation functions.</td>
</tr>
<tr>
<td>PMS Actuation Software/Hardware</td>
<td>RAW/CCF</td>
<td></td>
</tr>
<tr>
<td>System:  Passive Core Cooling System (PXS)</td>
<td>RAW/CCF</td>
<td>The IRWST injection lines /containment recirculation lines provide long-term core cooling following a LOCA. These screens are located inside the IRWST/containment and prevent large particles from being injected into the RCS. They are designed so that they will not be obstructed. In CAP1000 PSA model, the three IRWST screens are considered as one conservatively.</td>
</tr>
<tr>
<td>IRWST Screens, Containment Recirculation Screens</td>
<td>RAW/CCF</td>
<td></td>
</tr>
<tr>
<td>System:  Service Water System (SWS)</td>
<td>SD/RAW/CCF</td>
<td>These pumps and fans provide cooling of the CCS heat exchangers which is important to reduce the risk during shutdown conditions.</td>
</tr>
<tr>
<td>Service Water Pumps and Cooling Tower Fans</td>
<td>SD/RAW/CCF</td>
<td></td>
</tr>
</tbody>
</table>

Note: 1) RAW/CCF: the RAW is based on common cause failure of two or more of the specified SSCs

SD: shutdown

6. Discussion and Conclusions

The analyses for selecting critical human actions and risk-important human actions are performed based on CAP1000 PSA model. No critical human actions are found, and 20 risk-important human actions are obtained respectively. It is shown that human errors do not have significant influence on the plant safety due to the reduced dependency on human actions. The risk-important human actions should be fed back to the functional requirements and allocation analysts to confirm the reasonability and basis of allocating these tasks as human actions.

The risk-significant SSCs are selected based on CAP1000 PSA model. The selected risk-significant SSCs, together with those SSCs obtained by expert judgement or other considerations, are included in the D-RAP program and implemented using relevant QA programs.
7. References

