18.3 Functional Requirements Analysis and Function Allocation

Functional requirements analysis (FRA) is the identification and analysis of functions that must be performed in accordance with NUREG-0711 (Reference 1) to satisfy plant safety objectives (i.e., to prevent or mitigate the consequences of postulated accidents that could cause undue risk to the health and safety of the public).

Functional allocation (FA) is the analysis of the requirements for plant control and the assignment of control functions in accordance with References 1 and NUREG-0800 (Reference 2) for the following:

- Personnel (e.g., manual control).
- System elements (e.g., automatic control and passive, self-controlling phenomena).
- Combinations of personnel and system elements (e.g., shared control and automatic systems with manual backup).

18.3.1 Objectives and Scope

The purpose of the FRA and FA is to verify that plant safety functions have been defined and that the allocation of those functions to human and system resources has resulted in a role for personnel that takes advantage of human strengths and avoids human limitations (References 1 and 2).

All functions are considered in-scope in that they need to be captured and allocated. Particular significance is placed on functions that satisfy safety objectives (i.e., critical safety functions, as defined by NUREG-0696 (Reference 4)). Section 18.10 describes how procedure verification and validation (V&V) includes an explicit identification of functions to be performed to achieve plant safety objectives.

18.3.2 Functional Requirement Analysis Methodology and Results Summary

The U.S. EPR is an evolutionary PWR design based on years of operation and design experience from the precursor PWR plants (i.e., based on European N4 and Konvoi plants which are in turn based upon Westinghouse-designed PWRs currently operating in the U.S). The U.S. EPR also uses similar control of system functions and instrumentation and control (I&C) concepts as the predecessor PWRs and the Olkiluoto 3 (OL3) EPR.

Because the U.S. EPR evolved from previous PWR designs, the underlying nuclear and thermodynamic processes and most individual component functions for the U.S. EPR are inherited from the predecessor designs. During the early plant design stages for the OL3 EPR, process functions and their resulting functional requirements were derived from traditional PWR design principles established at the overall plant concept level. For screen-based human system interfaces (HSIs), functional

requirements are essentially translated into HSI controls and indications (i.e., screen elements). For the HSIs, applicable conceptual design inputs included:

- Concept of operations including the composition, the role of the operating staff, and the role of the control rooms.
- Definition of the automation criteria.
- Information needs and controls.

Descriptions of these design inputs are found in ANP-10279NP (Reference 3). HSI design principles, described in Section 18.7.6.1, are used to translate HSI design inputs into the HSI design.

The OL3 system engineers identified functions and their requirements in the (physical) system design documentation. The design control process procedures governed the detail required for identifying functional requirements. Those requirements initially included, as a minimum:

- Safety and design requirements.
- Role of the system.
- Functions of the system.
- Performance data (e.g., capacity, flow).
- Interfaces to other systems.
- I&C functions used to perform automatic safety functions.
- Principle requirements for operation from the main control room (MCR), from the remote shutdown station (RSS), or from a local control station (LCS).

Initial functional requirements were documented in system descriptions and used to develop successive levels of detail. OL3 system descriptions have organization and content similar to the system description documents developed for the U.S. EPR (see Section 5.3.4 of Reference 3). In order to complete OL3 system design documentation, system engineers performed FRA as they developed and translated the requirements for system performance into requirements for component or functional performance. This OL3 FRA included:

- Identification of operating modes:
  - Preparation and startup of the system.
  - Operation in the various plant states.

  - Switchover between operating modes, as applicable.
  - Periodic testing, if applicable.
  - Shutdown.
  - Fault conditions requiring automatic or operator response.

- Identification of:
  - Time criticalities, if any.
  - Parallel functions.
  - Availability of cues indicating the need to perform the task.
  - Availability of cues indicating successful completion of the task.

- Decisions on non-local control of components (e.g., motors, valves) via I&C (manual local operation is adequate if the component is only operated for preparation of startup under non-time-critical conditions or for maintenance such as isolation of sub-circuits).

- Analysis of the variables and check-back signals needed for:
  - Monitoring the operating conditions.
  - Controlling the process variables.
  - Monitoring the availability of the system.
  - Performing tests.
  - Trouble-shooting (diagnostics; evaluation of fault consequences).

Requirements for the design of the HSIs (including those for operation, maintenance, and testing) and for the associated work conditions were then derived from the characteristics of the identified tasks.

For the U.S. EPR, the functional requirements are translated from the OL3 system descriptions into the U.S. EPR system description documents taking into account changes in design principles and design requirements between the two EPR designs. Similarities between the U.S. EPR design and predecessor plants having extensive and successful operating histories provide a valid point of reference for evaluating changes and improvements to functional requirements. The U.S. EPR system description documents also provide the following:

- Safety classification of the function (including indicating critical safety functions).

- Design basis for the function.
- Plant modes or conditions when the function is required to be operable.
- Signals and corresponding actuators used to perform the function.
- Applicable setpoints for the function.

The FRA report included with the U.S. EPR V&V documentation lists the functions that were considered in-scope for meeting plant safety objectives. The FRA report also includes details of the differences between functional requirements for the OL3 EPR and the U.S. EPR for the 'safety functions', as well as the technical justification and design basis for each difference.

Functional requirements are maintained within the system description documents over the life of the plant as input to modification activities.

18.3.3 Functional Allocation Methodology and Results Summary

In the U.S. EPR design process, control of plant process functions is assigned and allocated to humans, automation, or a combination of human and automation using the set of automation criteria shown in Section 5.4.4.3 of Reference 3 and in the FA implementation plan. U.S. EPR plant process functions and certain control functions are allocated to closed-loop automatic control based on these automation criteria. Generally, functions automated in predecessor PWRs and in the OL3 EPR design are automated in the U.S. EPR design. Functions that are not automated are assigned to operators, either in the MCR or at LCSs. Any changes in automation are weighed against the total responsibilities of the operator to monitor automatic functions and to assume manual control during an automation system failure.

In addition to tabularizing system and component functions, each applicable system description document lists the type of control to which that function is allocated and the design basis for the allocation. A description of the personnel role with respect to functions and interfacing with automation is provided in the concept of operations (see Section 18.7.2).

A specific objective of the V&V is to verify that the automation design decisions have resulted in an interface that permits accomplishment of the safety functions within human capabilities and identifies as human engineering discrepancies (HEDs) any ineffective function allocation observed. This V&V approach verifies that the FA uses human strengths and avoids human limitations (Reference 2).

The FA report included in the V&V documentation:

- Details the complete set of automation criteria used for the U.S. EPR including the established control hierarchy between automatic and manual actions.

- Lists the functions that are automated for predecessor EPRs and the differences between the predecessors and the U.S. EPR.

- Explains the technical justification for each difference in functional allocation.

18.3.4 Changes to Functional Analysis or Allocation

As the U.S. EPR design evolves, functions may be re-allocated in an iterative manner in response to developing design specifics, operating experience, and the outcome of analyses and industry research. As described in Section 18.12, changes and modifications to the initial HSI configuration are required to be evaluated for impact to FRA or FA design documentation. The complete set of automation criteria and other design documentation previously described are considered as part of any proposed change or modification.

18.3.5 References

1. NUREG-0711, "Human Factors Engineering Program Review Model," Revision 2, U.S. Nuclear Regulatory Commission, 2004.

2. NUREG-0800, Chapter 18, "Human Factors Engineering," Revision 2, U.S. Nuclear Regulatory Commission, 2004.

3. ANP-10279P, "U.S. EPR Human Factors Engineering Program," AREVA NP Inc, January 2007.

4. NUREG-0696, "Functional Criteria for Emergency Response Facilities," U.S. Nuclear Regulatory Commission, 1981.

Next File