

18.3 Functional Requirements Analysis and Functional 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 this implementation plan is to establish methods, criteria and guidance for functional requirements analysis (FRA) and function allocation (FA) for the U.S. EPR plant design. The FRA identifies those functions that must be performed to satisfy plant safety and power generation objectives. This plan also describes how those defined functions are allocated among systems and trains, to automatic, group-level, and component-level control to meet regulatory requirements. The plan also uses FA to capitalize on human abilities and promote situational awareness. (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)).

18.3.2 Functional Requirement Analysis Methodology and Results Summary

FRA is divided into plant functions and system functions as described in the FRA/FA implementation plan (Reference 3). The plant-level FRA (PFRA) starts with plant-level safety (and power generation goals), continues to safety functions (and power generating functions), and ends with defined system functions. The system-level FRA (SFRA) begins with system functions, continues to train/subsystem functions and ends with component functions and support requirements. Both PFRA and SFRA consider system interdependence, interaction, diversity, and defense-in-depth. The plant-level and system-level FRA can be performed concurrently.

PFRA and SFRA are reconciled into a unified FRA by system function gap analysis (SFGA). During this process, system functions generated independently by PFRA and

SFRA are mapped to one another. The functional relationships between plant functions and system functions are then reconciled. The output of SFGA confirms that plant design goals are met by incorporating the differences as design inputs.

Critical safety functions are allocated to systems as guided by generic design criteria. Plant systems configurations or success paths that are responsible for or capable of carrying out the function are defined for all Technical Specification modes. The functional composition addresses the following levels:

- Plant safety functions (maintain fission product barriers).
- Critical safety functions (maintain reactor coolant inventory).
- System functions (control reactivity with boron/control rods).
- Specific plant sub-systems, structures, and components (in-containment refueling water storage tank (IRWST)).

Plant-level function description and mapping include:

- Purpose of the function.
- Conditions that indicate that the function can or should be initiated (loss of subcooling).
- Parameters that confirm system functions (e.g., flow, valve position, pump status).
- Parameters that confirm plant-level functions (e.g., reactor vessel level, core exit temperature).
- Parameters that indicate that functions can or should be terminated.
- Function diversity.
- Defense-in-depth in safety-related systems.

Plant system and component function description mapping include:

- System design document coordination.
- Review of system functions needed to perform high level goals.
- Parameters required to initiate, monitor, and terminate functions of that system.
- Disclosure of requirements to enable functions.
- Account of conditions that system functions need.
- Evaluation of all mode dependencies.

Plant function documentation is reviewed through the completion of the functional analysis, which includes operating modes as documented in Chapter 16. PRA and HRA analysis combined with OE documentation is used in various steps of the process. Updates and additions to the FRA are implemented during task analysis through the same process.

The FRA report 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 predecessor EPRs and the U.S. EPR for the ‘safety functions’, as well as the technical justification and design basis for each difference.

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 a set of automation criteria. 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 HFE Program Management Plan (Reference 5) concept of operations (see Section 18.7.2).

A specific objective of the V&V is to validate 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 includes:

- List of allocated functions for U.S. EPR
- List of differences and similarities between predecessor EPR and the U.S. EPR.
- Explains the technical justification for each difference in functional automation.

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. See Reference 3.

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. [*U.S. EPR Functional Requirements and Functional Allocation Implementation Plan, AREVA NP Inc., 2010.*]*
4. NUREG-0696, "Functional Criteria for Emergency Response Facilities," U.S. Nuclear Regulatory Commission, 1981.
5. [*U.S. EPR HFE Program Management Plan, AREVA NP Inc., 2010.*]*