GE Hitachi Nuclear Energy

NEDO-34182
Revision B
July 2025

US Protective Marking: Non-Proprietary Information
UK Protective Marking: Not Protectively Marked

BWRX-300 UK Generic Design Assessment (GDA) Chapter 15.4 – Safety Analysis – Human Actions

US Protective Marking: Non-Proprietary Information
UK Protective Marking: Not Protectively Marked

NEDO-34182 Revision B

INFORMATION NOTICE

This document does not contain proprietary information and carries the notations “US Protective Marking: Non-Proprietary Information” and “UK Protective Marking: Not Protectively Marked.”

IMPORTANT NOTICE REGARDING CONTENTS OF THIS REPORT
Please Read Carefully

The design, engineering, and other information contained in this document is furnished for the purpose of obtaining the applicable Nuclear Regulatory Authority review and determination of acceptability for use for the BWRX-300 design and licensing basis information contained herein. The only undertakings of GEH with respect to information in this document are contained in the contracts between GEH and its customers or participating utilities, and nothing contained in this document shall be construed as changing those contracts. The use of this information by anyone for any purpose other than that for which it is intended is not authorized; and with respect to any unauthorized use, no representation or warranty is provided, nor any assumption of liability is to be inferred as to the completeness, accuracy, or usefulness of the information contained in this document. Furnishing this document does not convey any license, express or implied, to use any patented invention or any proprietary information of GEH, its customers or other third parties disclosed herein or any right to publish the document without prior written permission of GEH, its customers or other third parties.

UK SENSITIVE NUCLEAR INFORMATION, UK EXPORT CONTROL AND US EXPORT CONTROL INFORMATION

This document does not contain any UK Sensitive Nuclear Information (SNI) subject to protection from public disclosure as described in the Nuclear Industries Security Regulations (NISR) 2003, does not contain UK Export Controlled Information (ECI), and does not contain US Export Controlled Information (ECI) subject to the export control laws and regulations of the United States, including 10 CFR Part 810.

EXECUTIVE SUMMARY

The BWRX-300 Generic Design Assessment (GDA) Preliminary Safety Report (PSR) Subchapter 15.4 presents the approach to the important human actions identified within the safety analysis for the BWRX-300. It demonstrates the adequacy of the treatment of these important human actions within the safety analysis.

The BWRX-300 Safety Strategy in conjunction with the BWRX-300 Human Factors Engineering (HFE) program aim to reduce the risks and consequences related to human interactions with the plant throughout all phases of the lifecycle. Important human actions are defined as human-machine interactions identified in the safety analysis. They encompass:

- Human actions which cause postulated initiating events.
- Pre-initiator human actions which do not directly cause an initiating event but adversely affect the progression of the resultant fault sequence.
- Post-initiator human actions modelled in the Probabilistic Safety Assessment (PSA).
- Human actions that are credited in the BWRX-300 Deterministic Safety Analysis (DSA).
- Human actions that are not credited in the DSA, but which are reflected as Defence Line (DL) 1 provisions in Baseline Deterministic Safety Analysis (BL-DSA) fault sequences as mitigation.
- Human actions reflected as DL1 provisions for prevention of initiating events.

Subchapter 15.4 describes the approach to identification, modelling, and substantiation of these important human actions. However, it is not the intention for the PSR to provide detailed substantive analysis of the important human actions. That analysis will be developed later in the safety analysis program. Other human-machine interactions are addressed via the HFE Program as described in PSR Chapter 18.

The content for this PSR subchapter reflects the level of maturity of the HFE Program, plant design, and safety analyses at the time of submission.

Claims and arguments relevant to GDA Step 2 objectives and scope are summarised in Appendix A, along with a statement regarding the reduction of risk such that it is As Low As Reasonably Practicable (ALARP). Appendix B provides a Forward Action Plan.

ACRONYMS AND ABBREVIATIONS

Acronym	Explanation
ALARP	As Low As Reasonably Practicable
ANS	American Nuclear Society
AOO	Anticipated Operational Occurrences
ASME	American Society of Mechanical Engineers
BL-DSA	Baseline Deterministic Safety Analysis
CAE	Claims, Arguments and Evidence
CBDTM	Cause-Based Decision Tree Method
CCA	Coping Capability Analysis
CN-DSA	Conservative Deterministic Safety Analysis
DBA	Design Basis Accident
DEC	Design Extension Condition
DL	Defence Line
DL1	Defence Line 1
DL2	Defence Line 2
DL3	Defence Line 3
DL4a	Defence Line 4a
DL4b	Defence Line 4b
DSA	Deterministic Safety Analysis
EX-DSA	Extended Deterministic Safety Analysis
EPRI	Electrical Power Research Institute
FFA	Functional Failure Analysis
FSF	Fundamental Safety Function
FPIE	Full Power Internal Events
GDA	Generic Design Assessment
GEH	GE Hitachi Nuclear Energy
HBSC	Human Based Safety Claims
HCR	Human Cognitive Reliability
HEA	Human Error Analysis
HEP	Human Error Probability
HF	Human Factors
HFE	Human Factors Engineering
HFEA	Human Failure Event Analysis
HFEITS	Human Factors Engineering Issues Tracking System
HFEPP	Human Factors Engineering Program Plan
HOHE	Human Operation Hazard Evaluation
HMI	Human-Machine Interface

Acronym	Explanation
HRA	Human Reliability Assessment
HSRC	Human Safety and Reliability Claim
I&C	Instrumentation and Control
IAEA	International Atomic Energy Agency
ISV	Integrated System Validation
LfE	Learning from Experience
LPSD	Low Power Shutdown
OE	Operating Experience
ONR	Office for Nuclear Regulation
OPEX	Operational Experience
ORE	Operator Reactor Experiments
PCSR	Pre-Construction Safety report
PIE	Postulated Initiating Event
PSA	Probabilistic Safety Assessment
PSR	Preliminary Safety Report
RAW	Risk Achievement Worth
RGP	Relevant Good Practice
RIF	Risk Increase Factor
SAA	Severe Accident Analysis
SCDS	Safety Case Development Strategy
SSCs	Structures, Systems and Components
THERP	Technique for Human Error Rate Prediction
TSM	Technical Specification Monitor
UK	United Kingdom
V&V	Verification and Validation

SYMBOLS AND DEFINITIONS

Symbol	Definition
Not Applicable	Not Applicable

Term	Definition
Anticipated Operational Occurrences	A frequency category applied to Postulated Initiating Event (PIEs) or event sequences with frequencies of occurrence greater than or equal to 1.0E-02 per reactor-year.
Design Basis Accident	A frequency category applied to PIEs or event sequences that are expected to occur at a frequency between 1.0E-02 and 1.0E-05 per reactor year.
Design Extension Conditions	A frequency category applied to PIEs or event sequences with frequencies of occurrence less than 1.0E-05 per reactor-year.
Deterministic Safety Analysis	Safety analysis using, for key parameters, single numerical values (taken to have a probability of 1), leading to a single value for the result. Typically used with either best estimate or conservative values, based on expert judgement and knowledge of the phenomena being modelled.
Fundamental Safety Functions	The highest-level objectives that must be delivered during both normal operation and under accident conditions. Under accident conditions, the circumstances are likely to be such that control of one or more functions has been lost. However, the same fundamental objectives remain.
Important Human Action	An important human action is a human-machine interaction identified in the safety analysis. Important human actions encompass: • Human actions which cause postulated initiating events. • Pre-initiator human actions which do not directly cause an initiating event but adversely affect the progression of the resultant fault sequence. • Post-initiator human actions modelled in the PSA. • Human actions that are credited in the BWRX-300 DSA. • Human actions that are not credited in the DSA, but which are reflected as DL1 provisions in BL-DSA fault sequences as mitigation. • Human actions reflected as DL1 provisions for prevention of initiating events
Human Factors Engineering	The application of knowledge about human capabilities and limitations to plant, system, and equipment design. Human Factors Engineering (HFE) ensures that the plant, system, or equipment design, tasks, and work environment are compatible with the sensory, perceptual, cognitive, and physical attributes of the personnel who operate, maintain, and support it.
Human Factors Engineering Verification and Validation	HFE Verification and Validation (V&V) evaluates completed design features including alarms, controls, indications, and their associated hardware. During HFE V&V, design features are compared with regulatory requirements and guidance, HFE requirements, and the requirements generated during analysis of operator tasks. HFE V&V consists of design verification, task support verification, and Integrated System Validation (ISV).

Term	Definition
Human Factors Issue	A problem or finding that is known to the industry or is identified throughout the life cycle of the HFE aspects of design, development, and evaluation. Issues are items that need to be addressed later and are tracked to ensure they are not overlooked.
Human Safety and Reliability Claim	An explicit or implicit statement in the safety analysis regarding HFs and/or human performance which needs to be demonstrated to be supported by fact (i.e., substantiated) for assurance that the analysis conclusions are tenable.
Normal Operation	Operation within specified operational limits and conditions. This includes startup, power operation, shutting down, shutdown, maintenance, testing and refuelling.
Operational Experience (OPEX)	Operating experience is the collection and dissemination of knowledge gained via the operation of nuclear facilities. It often includes descriptions of actual events and near-misses and how they were identified and resolved with the objective of preventing future recurrence.
Postulated Initiating Event	A change in state of plant equipment, caused by hazards such as equipment failures and internal/external events, that impacts the performance of a Fundamental Safety Function (FSF) and requires mitigation by DL functions.
Probabilistic Safety Assessment	A comprehensive, structured approach to identifying failure sequences, constituting a conceptual and mathematical tool for deriving numerical estimates of risk.
Severe Accident Analysis	Safety analysis focused on mitigating the consequences of core damage events.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

None.

REVISION SUMMARY

Revision #	Section Modified	Revision Summary
A	All	Initial Revision
B	Various	Update for end of Step 2 Consolidation

15.4 HUMAN ACTIONS

Introduction

This Preliminary Safety Report (PSR) subchapter presents the approach to the identification, assessment and substantiation of the important human actions identified within the safety analysis for the BWRX-300. It demonstrates the adequacy of the treatment of these important human actions within the safety analysis.

The content of this PSR subchapter reflects the level of maturity of the HFE program, plant design, and safety analyses at the time of submission.

Subchapter Structure

The subchapter covers the following elements:

- The proportionate/graded approach to important human actions
- Identification of important human actions
- Important human actions relating to pre-initiators, initiating events and post-fault actions
- Human reliability assessment and the progressive substantiation of important human actions
- Important human actions in the DSA
- Important human actions in the PSA.

Interfaces with Other Chapters

The Subchapter 15.4 PSR interfacing chapters/subchapters are listed below. This includes main interfaces, which are the topics most closely connected with Subchapter 15.4 at the current stage of the design and safety case.

Main Interfaces:

- Chapter 18 - Human Factors Engineering, NEDC-34190P, “BWRX-300 UK GDA Chapter 18: Human Factors Engineering,” (Reference 15.4-1) discusses the HFE program for the BWRX-300 and demonstrates the adequacy of integration of HFE requirements and analysis results into the plant design. Subsection 18.2.5 addresses the treatment of important human interactions with the plant in general. It highlights how human actions are addressed within the HFE program in general and provides the link to Subchapter 15.4.
- Chapter 3A - Safety Objectives and Design Rules for SSCs, NEDC-34165P, “Chapter 3A: Safety Objectives and Design Rules for SSCs” (Reference 15.4-2), describes the BWRX 300 general design principles and processes. It summarises measures and assessments to ensure safety, including human factors. This chapter provides the radiological acceptance principles and criteria. Subchapter 15.4 describes how important human actions are incorporated into the safety analysis for the BWRX-300.
- Subchapter 15.1 - General Considerations of the BWRX-300 Safety Analysis, NEDC-34179P, “Chapter 15.1: General Considerations of the BWRX-300 Safety Analysis,” (Reference 15.4-3) defines of the scope of the safety analysis and the approach adopted (i.e., conservative, or realistic, as appropriate) for each plant state, from normal operation to Design extension Conditions (DECs) with core melting. It defines the scope of the analysis for Subchapter 15.4.

- Subchapter 15.5 - Deterministic Safety Analysis, NEDC-34183P, “BWRX-300 UK GDA Chapter 15.5: Deterministic Safety Analyses,” (Reference 15.4-4) defines initiating faults and hazards that are reasonably foreseeable, conservatively justifies accident sequences that follow those faults and hazards and assesses the design against engineering principles. It defines where important human actions are credited within the DSA. In doing so it provides a key input to Subchapter 15.4, which deals with the analysis of those important human actions.
- Subchapter 15.6 - Probabilistic Safety Assessment, NEDC-34184P, “BWRX-300 UK GDA Chapter 15.6: Probabilistic Safety Assessment,” (Reference 15.4-5) defines the approach to implementing a PSA that supports risk-informed design development. This enables an understanding of the overall risk and any dominant contributors. The PSA also provides essential understanding of strengths and weaknesses of the design with complex systems and interdependencies. The important human actions and human reliability assessment described in Subchapter 15.4 are integral parts of the PSA.
- Subchapter 15.7 – Internal Hazards, NEDC-34185P, “BWRX-300 UK GDA Chapter 15.7: Internal Hazards,” (Reference 15.4-6) defines the approach to internal hazards and where important human actions may be credited in the safety analysis.
- Subchapter 15.8 – External Hazards, NEDC-34186P, “BWRX-300 UK GDA Chapter 15.8: External Hazards,” (Reference 15.4-7) defines the approach to external hazards and where important human actions may be credited in the safety analysis.

Other Chapter Interfaces:

- Chapter 13 - Conduct of Operations, NEDC-34176P, “BWRX-300 UK GDA Chapter 13: Conduct of Operations,” (Reference 15.4-8) describes the BWRX-300 organizational structure, staffing and procedures, including the use of Human Factors (HF) methods and guidance in their future development. These operational aspects provide the context for the important human actions considered in Subchapter 15.4.
- Chapter 19 - Emergency Arrangements, NEDC-34191P, “BWRX-300 UK GDA Chapter 19: Emergency Preparedness and Response,” (Reference 15.4.9) covers elements of the BWRX-300 design that will facilitate on-site and off-site emergency arrangements. Subchapter 15.4 deals with the analysis of important human actions claimed in severe accidents and informs emergency preparations.
- Chapter 27 – ALARP Evaluation, NEDC-34199P, “BWRX-300 UK GDA Chapter 27: ALARP Evaluation,” (Reference 15.4-10) provides the ALARP demonstration for the BWRX-300. Subchapter 15.4 contributes to ALARP arguments in relation to the potential for human error.

Claims and arguments relevant to GDA Step 2 objectives and scope are summarised in Appendix A, along with a statement regarding the reduction of risk such that it is As Low As Reasonably Practicable (ALARP). Appendix B provides a Forward Action Plan.

15.4.1 General Considerations

The overall goal of the BWRX-300 HFE program is to control the risks arising from human interactions with the plant (005N1716, "BWRX-300 Human Factors Engineering Program Plan," (HFEPP) (Reference 15.4-11) and PSR Chapter 18 (Reference 15.4-1)). In doing so, the program gives consideration to human-machine interactions that occur during construction, commissioning, decommissioning, normal operations, and outages (refuelling and maintenance outages, including extended refurbishments), as well as in abnormal, emergency, and accident conditions.

The subset of the human-machine interactions that relate to nuclear safety are referred to generally as "important human actions." Important human actions are identified in the safety analysis and encompass:

- Human actions which cause postulated initiating events.
- Pre-initiator human actions which do not directly cause an initiating event but adversely affect the progression of the resultant fault sequence.
- Post-initiator human actions modelled in the Probabilistic Safety Assessment (PSA).
- Human actions that are credited in the BWRX-300 Deterministic Safety Analysis (DSA).
- Human actions that are not credited in the DSA, but which are reflected as Defence Line (DL) 1 provisions in Baseline Deterministic Safety Analysis (BL-DSA) fault sequences as mitigation.
- Human actions reflected as DL1 provisions for prevention of initiating events.

Within the nuclear industry these human actions may also be referred to as Human Based Safety Claims (HBSC), usually in relation to claims on operator action made within the DSA or human failure events (usually in relation to the PSA). Subchapter 15.4 describes the approach to identification, modelling and substantiation of important human actions identified in the safety analysis. Other human-machine interactions are addressed via 005N1716, "BWRX-300 Human Factors Engineering Program Plan," (HFEPP) (Reference 15.4-11) as discussed in PSR Chapter 18.

As human-machine interactions are a central focus of the HFE program, the methodologies, tools, and activities described in PSR Chapter 18 directly address important human actions in the following ways:

- The decisions regarding the allocation of functions provide the first step in applying a hierarchy of controls and eliminating important human actions that may not be feasible or performed reliably PSR Chapter 18, Section 18.2.3.
- 005N3747, "Human Factors Engineering Concept of Operation for BWRX-300," (Reference 15.4-12) provides the overarching context for the important human actions.
- Learning from OPEX relating to predecessor designs is taken into account. This informs the design of similar important human actions identified for the BWRX-300 (PSR Chapter 18, Section 18.2.1). OPEX also informs the application of a hierarchy of controls and the decisions on whether important human actions should be eliminated.
- The use of task analysis (including link analysis, timeline analysis, and preliminary workload analysis) informs the development of the important human actions. It also provides evidence substantiating the important human actions and any associated human error probabilities (refer to Section 15.4.1.5).

- The iterative HFE design activities address performance influencing factors that could undermine reliable completion of the important human actions. These design activities include the development of requirements (PSR Chapter 18, Section 18.2.2), the application of codes and standards (PSR Chapter 18, Section 18.2.2), and testing and evaluation (refer to PSR Chapter 18, Section 18.3.4).
- Issues that are identified in relation to the design and substantiation of important human actions are managed via the Human Factors Engineering Issues Tracking System (HFEITS), PSR Chapter 18, (refer to Section 18.1.5).
- Evidence supporting the substantiation of important human actions is provided by Integrated System Validation (ISV). HFE Validation ensures that the design, particularly the HFE-specified aspects, accomplishes its intended goals for usability and reducing the risk of human error to as low as reasonably achievable.

15.4.1.1 Proportionate/Graded Approach

The HFE Program takes a proportionate approach to the design and substantiation of human actions based on their level of risk (PSR Chapter 18, Section 18.1.5 and 005N1716 (Reference 15.4-11)). The human actions will be assigned risk levels based on the following principles:

- Any important human actions that are credited in the DSA will be assigned a high-risk level
- Where the PSA identifies important human actions as being risk significant based on measures of risk importance these will also be assigned a high-risk level
- The remainder of the important human actions modelled in the PSA will be assigned a medium-risk level. The risk level determines the HFE application level that will be applied to the human action and the HFE application level defines the graded work scope

At present, no important human actions are credited in the DSA. The evaluation of important human actions is an ongoing process conducted in an iterative manner throughout the system design lifecycle. If future iterations of the DSA do credit human actions, the Risk Levels will be assessed. They will then be re-assessed for changes with each subsequent revision of the DSA. Similarly, if important human actions are identified in the PSA, the risk levels will be assessed and then re-assessed with each subsequent revision.

In relation to the design, additional reviews of the appropriateness of the HFE application level will be undertaken for each human action by considering:

- Complexity of the action
- Anticipated complexity and constraints of the Human-Machine Interface (HMI)
- Complexity of the system
- Frequency of the task
- Physical environment
- Cognitive environment
- Novelty of the action, system, or HMI technology
- Time sensitivity of the action

This ensures an appropriate and integrated treatment of the important human actions both in the safety analysis and in the design.

15.4.1.2 Human Actions and Postulated Initiating Events

The Postulated Initiating Events (PIEs) are inputs to both the DSA and PSA. The PIEs are identified from the plant level failure analysis. The design is subject to two types of plant-level failure analysis, 006N5064, "BWRX-300 Safety Strategy," (Reference 15.4-13):

- Functional Failure Analysis (FFA). The FFA identifies failures of plant systems or equipment with potential to cause a PIE that challenges a Fundamental Safety Function (FSF)
- Human Failure Event Analysis (HFEA)

The primary objective of the two failure analyses is to systematically and comprehensively identify Structures, Systems, and Components (SSCs) functional and human failures that have potential to initiate a PIE, or to initiate or worsen a hazard that leads to a PIE.

The HFEA is intended to identify failures that involve a single human failure event that could potentially lead to a PIE. The HFEA was previously referred to as the Human Operation Hazard Evaluation, (HOHE). Human actions that can lead to a PIE are referred to as Type B important human actions (or more generally within the nuclear industry, Type B HBSCs or human failure events).

Type B important human actions are those that could potentially initiate an abnormal or accident event sequence; they primarily involve:

- Errors made by personnel during normal operations while changing the state of plant equipment from a designated control location, where the change in state is performed incorrectly
- Errors by personnel during a planned maintenance activity resulting in an unintended change in the state of plant equipment

The purpose of the HFEA is to identify plausible and relevant Type B important human actions, including understanding their underlying error mechanisms. As failure of Type B important human actions result in incorrect and undesired plant equipment state changes, failure of many of these important human actions result in equipment failures that are already included in the FFA. Additionally, failure of some Type B important human actions, particularly the maintenance-related ones, may result in an internal hazard already included in the internal hazard evaluation. Specifically identifying the potential human "initiation" of these failures and hazards, ensures consideration of the human error causes, leads to more realistic frequency estimation, and informs other aspects of the design, specifically the HMIs. The HFEA also aims to identify unique "new" human-initiated failures that may not be included in or identified by other analyses.

The scope of the HFEA is limited to single human failure events. By definition, a single human failure event encompasses the multiple human error mechanisms required to impact the plant in the postulated manner, i.e., failure of an important human action includes the error(s) in decision-making and the error(s) in action of a set of grouped cognitive and physical activities that comprise the failure of a task in such a way it causes the incorrect and undesired plant equipment state change.

The HFEA scope does not include violations (intentional, but non-malicious, performance of actions in direct non-compliance with documented procedures), or malicious acts. These are addressed within the site licensing phase. However, the potential for the design to induce violations through inefficient layout of equipment is considered by the broader HFE program (see Appendix B, Forward Action PSR15.4-189).

The HFEA analysis to date has not identified any important human actions that would cause an initiating event that would not already be covered by the general transient occurrence data

(see Appendix B, Forward Action PSR15.4-192). If any Type B important human actions are identified during future iterations of the HFEA, 007N3073, "BWRX-300 Human Operation Hazard Evaluation," (Reference 15.4-14) they will result in:

- Incorporation of the relevant important human actions into the PSA model and/or deterministic PIE selection as appropriate
- Design issues being entered into the HFEITS for resolution

15.4.1.3 Identification of Pre-Initiator and Post-Fault Human Actions

The pre-initiator and post-fault important human actions are established by the safety analysis, either explicitly or implicitly (also referred to within the nuclear industry as Type A and Type C important human actions or HBSCs/human failure events respectively).

The important human actions will be identified through review of the following safety analyses (see Appendix B, Forward Action PSR15.4-191):

- Functional failure hazard evaluation (i.e., Failure Mode and Effects Analysis)
- External and internal hazard evaluation
- Fault evaluation
- PSA
  - Internal events at-power
  - Low power and shut down events
  - Spent fuel pool events
  - Fuel and heavy load movements PSA
  - Human reliability assessment
  - Level 2 PSA, Severe Accident Analysis (SAA)
- DSA
- Fire safe shutdown analysis
- Reliability evaluation and modelling (i.e., consideration of reliability, availability, maintainability and inspectability).

15.4.1.4 Human Safety and Reliability Claims Database

The important human actions, along with the basis, context, and summary of substantiating evidence, are documented in the Human Safety and Reliability Claim (HSRC) database for tracking and future substantiation (005N1716 and 007N3447 (References 15.4-11 and 15.4-15)). The specific claims are reproduced verbatim wherever possible to limit the possibility for misinterpretation.

The HSRCs will be organised into three categories (these are related to the way in which the HSRCs are substantiated, not to their risk significance):

- Category 1 - Human performance claims for human action credited in the DSA for event mitigation (e.g., task performance time) and associated assumptions
- Category 2 – Human Error Probability (HEP) quantifications for human failure events modelled in the PSA and associated assumptions
- Category 3 - All other claims (e.g., assumptions regarding particular procedures or alarms, generally made to support qualitative human performance claims)

The database will capture all the important human actions claimed in the safety analyses, as well as the source of the claim, their key characteristics, the related assumptions, and any associated HMIs. This ensures visibility of the important human actions. It also enables clear links to the design activities to be established, and managed.

15.4.1.5 Substantiation of Claims on Important Human Actions through Qualitative Human Error Analysis

Qualitative Human Error Analysis (HEA) is conducted for all claims on Category 1 important human actions and all claims on risk-significant Category 2 important human actions (using the risk importance measure: Fussell-Vesely (FV) ≥ 0.20), with the following objectives (007N3447 (Reference 15.4-15), also see Appendix B, Forward Action PSR15.4-185):

- For claims on Category 1 important human actions (credited in DSA) – the HEA aims to demonstrate the operator action is achievable with a high degree of confidence.
- For claims on Category 2 important human actions (quantified human failure events) – the HEA supports the characterisation used to quantify the HEP for risk-important human actions, including the selection of performance influencing factors or dependencies.

The HEA involves undertaking a risk-proportionate level of task analysis. Task analysis is undertaken in accordance with the methodology summarised in the HFEPP (005N1716 (Reference 15.4-11)) and detailed in the Human Factors Engineering Safety Analysis (007N3447 (Reference 15.4-15)).

Substantiation of the important human actions occurs in an iterative and progressive manner as the fidelity increases during the system lifecycle. This will culminate in validation of the important human actions once the design and safety case have reached maturity.

15.4.2 Human Actions in Deterministic Safety Analysis

15.4.2.1 Overview

The BWRX-300 Safety Strategy defines the approach to DSA, 006N5064 (Reference 15.4-13). There are five 'layers' of DSA: Baseline Deterministic Safety Analysis (BL-DSA), Conservative Deterministic Safety Analysis (CN-DSA), Extended Deterministic Safety Analysis (EX-DSA), Coping Capability Analysis (CCA) and SAA. The mapping of the functional Defence Lines (DLs) to these analyses is summarised in Section 2.1.4 of 006N5064 (Reference 15.4-13).

At present, there are no important human actions credited in the functional Defence Line 2 (DL2), Defence Line 3 (DL3), Defence Line 4a (DL4a), Defence Line 4b (DL4b) that are analysed in the five 'layers' of the DSA. The Licensing Topical Report (LTR) 006N5064 (Reference 15.4-13) places specific constraints on when important human actions may be credited within the DSA. These constraints are described in the following sections. The treatment of important human actions associated with PIEs that provide an input to the DSA as discussed in Section 15.4.1.2 above.

15.4.2.2 Baseline Deterministic Safety Analysis

The scope of BL-DSA includes Anticipated Operational Occurrences (AOOs) and Design Basis Accident (DBA) PIEs. These are selected through the Deterministic PIE Selection portion of the Fault Evaluation process in 006N5064 (Reference 15.4-13). This includes AOO PIEs caused by a single important human action failure.

The primary objective for the BL-DSA is to model the expected plant response to AOO and DBA PIEs assuming all functions, regardless of safety category, are available to respond as designed to mitigate the event (excepting those failed as part of PIE initiation or by consequence of the PIE). Best estimate or realistic analysis conditions are used, and the results are compared to deterministic acceptance criteria based on the event category determined for the PIE in the fault evaluation.

As the BL-DSA documents the expected response of the plant, it can reflect important human actions when it is reasonable (in terms of time to diagnose and respond, availability of indications supporting diagnosis, and availability of systems to carry out the action given the scenario) for them to be part of the expected response. This is particularly the case for relatively slow-moving plant transients, and for PIEs initiated when operators are already actively involved in manual control of the plant processes. If it is identified that a PIE could result from a human error during manual control actions, the analysis can reflect personnel correcting the error allowing the action to be successful. This can be reflected without need for extended time to perform the action and recovery, because the person performing the action is already actively engaged, subject to appropriate analysis of the recovery actions, (e.g., taking account of any dependency coupling mechanisms between the initiating error and the recovery action.

If any important human actions are captured in future iterations of the BL-DSA:

- Confirmation will be sought that if the actions were not taken, the acceptance criteria associated with the event category of the PIE would be satisfied
- The important human actions will be identified as DL1 provisions to be included in the plant operating procedures
- A CN-DSA event sequence stemming from the same PIE will be analysed assuming no important human actions

Any important human actions captured in future iterations of the BL-DSA will support the development of operating procedures for off-normal conditions and the minimisation of

avoidable duty-cycles on plant equipment that supports automatic DL function actuations. Both of these would contribute to the robustness of DL1 provisions for the plant design and its operation (refer to 006N5064 (Reference 15.4-13)).

15.4.2.3 Conservative Deterministic Safety Analysis

The scope of CN-DSA includes AOO and DBA PIEs selected through the deterministic PIE selection portion of the fault evaluation process, with additional mitigation failures assumed (to form event sequences) compared to the BL-DSA analysis of the same PIEs. This could include AOO PIEs caused by failure of a single important human action.

The primary objective for the CN-DSA is to demonstrate capability to mitigate AOO and DBA PIEs and event sequences crediting only DL3 functions and inherent or passive safety features. It provides the formal demonstration of the plant's capability to maintain performance of the FSFs for a 72-hour period crediting only passive functionality and Safety Class 1 equipment. Therefore, crediting of human actions to perform a FSF is not permitted in CN-DSA.

15.4.2.4 Extended Deterministic Safety Analysis

The scope of EX-DSA includes all PIEs and event sequences assigned to the Design Extension Condition (DEC) event category selected through the deterministic PIE selection and complex sequence selection processes.

The primary objectives of the EX-DSA are to:

- Demonstrate an effective means of motive force for control rod insertion, diverse from hydraulic action
- Demonstrate a second functional DL against DBA PIEs for which DL3 functions were credited in both the BL-DSA and CN-DSA
- Demonstrate mitigation of PIEs in the DEC event category
- Demonstrate the capability of the plant to avoid core damage (severe accident conditions) in unlikely event scenarios involving combinations or types of mitigation failures that are beyond those deterministically postulated ('complex sequences')

Crediting of human actions to perform a FSF is not permitted in those DEC event sequences identified through the deterministic PIE selection process. Human actions are not credited in those EX-DSA event sequences identified through the complex sequence selection process. However, it may be allowable in exceptional cases to credit a human action in these sequences; in such cases a justification of impracticability for implementing an automatic function will be provided (refer to 006N5064 (Reference 15.4-13)).

15.4.2.5 Coping Capability Analysis

The scope of the CCA includes the event sequences selected through the coping capability sequence selection process (refer to 006N5064 (Reference 15.4-13)).

The objective of the CCA is to model time-extended plant response to the selected scenarios. It is the formal demonstration that the design supports seven days of coping capability using only installed systems with no reliance on significant human actions or external resources. In this context, "coping capability" refers to the ability to ensure the FSFs are maintained for seven days after an event resulting in reactor shutdown without the necessity of human action.

It is allowable to reflect simple human actions that are rule-based and require no complex cognitive or physical activity. Specifically, the following constraints apply:

- Simple monitoring of key parameters without decision-making or further actions required in response can be claimed

- Simple “automatic” rule-based actions that are not part of mitigating the sequence can be claimed. Such actions include:
  - Assessing the radiation environment in and around the plant in line with routine radiation protection assessment processes
  - Response to personnel hazard alarms, including relocation to a protected, habitable area if personnel are located in an area subject to conditions that cause it to become uninhabitable
  - Communicating plant conditions routinely with required parties, including plant public address announcements and interfacing with security and external parties as required

Examples of human actions that cannot be credited include:

- Actions to provide back-up to failed automatic DL functions
- Actions to reconfigure a process system (start/stop pumps or fans, open/close valves or dampers)
- Actions to reconfigure electrical systems (load shedding, reconfiguring of Instrumentation and Control (I&C) equipment)

15.4.2.6 Severe Accident Analysis

The scope of the SAA is defined by those event sequences selected through the SAA selection process. Accident progression analyses are performed to establish plant thermal-hydraulic behaviour, chronology of accident progression (the timing of the core damage and containment failure), and containment loads due to complex severe accident phenomena. This analysis includes models for the important accident phenomena that might occur in the reactor pressure vessel, in the containment, and in the reactor building. There is a strong relationship between the deterministic SAA modelling of severe accident sequence progression and the Level 2 PSA. Deterministic modelling is used to confirm that the Level 2 containment event categories and release categories are valid. As best-estimate analysis conditions are used in the SAA, human actions may be credited. If any human actions are credited, then the output of the SAA provides insights into the important human actions considered during the development of accident management procedures (refer to 006N5064 (Reference 15.4-13)).

15.4.2.7 Deterministic Hazard Analysis

Internal and external hazards are handled differently to PIEs that arise from SSC failures or human failure events. As any number of possible PIEs might result from a hazard, the evaluations do not attempt to postulate specific PIEs caused by the identified hazards. Instead, the outputs from the internal hazard evaluation and external hazard evaluation (i.e., expected frequencies versus the intensity) are fed directly into appropriate deterministic hazard analyses. The analyses will demonstrate that the plant design can withstand the hazards while maintaining performance of the FSFs.

The objective of these analyses is to demonstrate that protection is provided against all selected credible hazards and hazard sources/sub-sources through DL1 provisions within the design of the plant SSCs. DL1 provisions include operational programs that ensure the plant is operated within its analysed safety profile, and the operating procedures in place to support this. Administrative controls such as these are discussed within PSR Chapter 18, Section 18.2.5. They are not the focus of Subchapter 15.4. DL1 also includes operator actions reflected in the BL-DSA as DL1 provisions, though these are not explicitly identified in the “BWRX-300 Fault Evaluation and Fault List” (005N3558, Reference 15.4-16). Hence a forward action has been raised for their inclusion in this document (see Appendix B, Forward Action PSR15.4-361). In addition, operator actions reflected in the BL-DSA as DL1 provisions have

not been explicitly addressed within the HFE methodologies (e.g. 005N1716 “BWRX-300 Human Factors Engineering Program Plan” (Reference 15.4-11), 007N3447 “Human Factors Engineering Safety Analysis” (Reference 15.4-15)), hence a forward action has been raised for their inclusion (see Appendix B, Forward Action PSR15.4-362).

A control room habitability analysis will be performed to identify those scenarios that could challenge the ability of the operators to remain in the MCR and to confirm that the secondary control room will be habitable in the context of those scenarios. It also confirms that the equipment supporting requisite monitoring and operator control actions in the habitable location remain functional under the conditions associated with the scenario. This addresses a subset of the performance influencing factors that could impact important human actions in hazard scenarios.

The CCA imposes specific constraints regarding operator actions that can or cannot be credited to establish or extend habitability and operability of control/monitoring locations for the scenarios within its scope. These constraints will be applied during the control room habitability and operability analysis.

15.4.2.8 Operator Actions Not Credited in the Deterministic Safety Analysis

The BWRX-300 design is being developed in a manner that reduces the risk of human actions leading to PIEs and minimises reliance on important human actions following a PIE, consistent with both regulatory expectations for modern nuclear power plant designs and current industry good practice.

Where credit is not taken for human actions in the DSA, this does not mean that operators should not take action in such scenarios. Proper operator responses can lessen the severity of a scenario compared to the analysed demonstration cases and can, in relatively slow developing scenarios, prevent unnecessary challenges to the equipment ultimately relied on for safety. Therefore, the BWRX-300 Safety Strategy (006N5064 (Reference 15.4-13)) distinguishes between “credited” actions which are synonymous with HBSCs in the UK and actions that are “reflected” in the safety analyses. i.e. operator responses that are modelled in the safety analyses but are not “claimed” as they are not required to meet DSA acceptance criteria. These operator actions are “reflected” in certain specific cases, generally the Base Line (BL) DSA. Such actions are also typically associated with DL1 provisions to minimise the potential for failures and initiating events to occur in the first place and minimise the potential for failures to occur in DL functions. Such operator responses, and the operating procedures that guide them are therefore integral to the BWRX-300 Defence-in-Depth (D-in-D) concept. However, it should be highlighted that these operator actions are not “credited” as they are not required to meet the DSA acceptance criteria. As noted in Section 15.4.2.7 above, operator actions reflected in the BL-DSA as DL1 provisions are not explicitly identified in the “BWRX-300 Fault Evaluation and Fault List” (005N3558, Reference 15.4-16). Hence a forward action has been raised for their inclusion in this document (see Appendix B, Forward Action PSR15.4-361).

For these reasons, operator actions will be reflected in certain safety analyses, both deterministic and probabilistic, to gain understanding of when the actions can be beneficial and to inform operating procedure development. Additionally, in certain types of very low likelihood event sequences operator actions may be credited to support performance of FSFs. Examples include complex sequences involving failure to shut down the reactor and external hazards probabilistically combined with un-related, yet simultaneous common cause failures of systems protected from, and qualified for the hazard. PSR Subchapter 15.5 discusses the complex fault sequences and states whether any operator actions are credited or reflected in the analyses of these sequences.

It is recognised that errors of commission could occur when undertaking operator actions that are not credited in the DSA. Errors such as these could aggravate fault conditions. These

operator actions will be addressed by the PSA and through the general activities in the HFE program. If operator actions are reflected or credited in an analysis, they will be identified as HSRCs and will be demonstrated to be achievable to the required performance standards, see 006N5064 “BWRX-300 Safety Strategy” (Reference 15.4-13). The approach to elicitation and management of the HSRCs and how their achievability will be demonstrated is described in 007N3447, “Human Factors Engineering Safety Analysis Report,” (Reference 15.4-15).

15.4.2.9 Substantiation of Human Actions Claimed in the Deterministic Safety Analysis

If any human actions are credited in the DSA, their substantiation occurs in an iterative and progressive manner as the maturity of the design increases during the system lifecycle. This culminates in validation of the human actions once the design and safety case have reached maturity. Substantiation uses a risk-proportionate level of task and Human Error Analysis (HEA) (Section 15.4.1.5 and PSR Chapter 18, Section 18.2.4 and 005N1716 (Reference 15.4-11).

15.4.3 Human Actions in Probabilistic Safety Analysis

15.4.3.1 Overview

Two PSA levels are applied that provide estimates of overall risk to the surrounding population and environment:

- Level 1 estimates the first measure of risk (core damage frequency):
  - The scope of Level 1 PSA includes all plant operational modes (i.e., full power, low power, and shutdown) and considers events affecting both the reactor core and the spent fuel pool. It includes consideration of:
    - Internal events at-power
    - Low power and shut down events
    - Spent fuel pool events
    - Fuel and heavy load movements
- Level 2 estimates the second measure of risk (radioactivity release):
  - The scope of sequences evaluated in the Level 2 PSA corresponds to the core damage sequences developed in the Level 1 PSA
  - The primary objective of Level 2 PSA is to characterise the frequency, magnitude, timing, and other relevant characteristics of potential radioactive releases resulting from the core damage sequences
  - The Level 2 PSA interfaces with the SAA

A fundamental requirement of the Safety Strategy is to ensure that any claimed human actions are achievable and meet the performance requirements for the event sequences and scenarios in which they are claimed; (refer to 006N5064 (Reference 15.4-13)). As such, suitably scoped qualitative HEA and Human Reliability Assessment (HRA) will be performed in support of the safety strategy implementation and to inform the design through design-to-analysis requirements.

The objectives of the probabilistic HRA are to derive HEPs for selected important human actions determined by the PSA screening techniques to be risk-important to event sequences within the PSA. The HRA will also inform design improvements required to support the derived probabilities. Three types of important human action are defined for modelling in the PSA:

- Type A important human actions: Pre-initiators (refer to Section 15.4.1.3)
- Type B important human actions: Initiators (Section 15.4.1.2)
- Type C important human actions: Post-fault actions (Section 15.4.1.3)

Substantiation of the important human actions and associated HEPs occurs in an iterative and progressive manner (Section 15.4.1.5).

15.4.3.2 HRA Process

In relation to HRA, the aim is to conform with the guidance of the Relevant Good Practice (RGP) presented in:

- The American Society of Mechanical Engineers (ASME)/American Nuclear Society (ANS) RA-S-1.1-2022 “Standard for Level 1 /Large Early Release Probabilistic Risk Assessment for Nuclear Power plants” (Reference 15.4-17)

- International Atomic Energy Agency (IAEA)-TECDOC-1804, “Attributes of Fuell Scope Level 1 Probabilistic Safety Assessment for Application in Nuclear Power Plants,” (Reference 15.4-18)
- UK Office for Nuclear Regulation (ONR) NS-TAST-GD-063, “Technical Assessment Guide: Human Reliability Analysis,” (Reference 15.4-19)

The HRA process uses resources from the Electrical Power Research Institute (EPRI) suite of HRA tools. The general HRA process follows the steps outlined in EPRI-NP-3583, “Systematic Human Action Reliability Procedure,” (Reference 15.4-20). For the Level 1 PSA this involves:

- Identification of human-interactions
- Capturing key assumptions
- Focusing on the key interactions through screening
- Describing the human actions in detail
- Incorporating performance influencing factors
- Quantifying the HEPs

In relation to the Type A human actions, screening criteria from ASME HR-B1 of the ASME Level 1 PSA Standard, RA-S-1.1-2022 (Reference 15.4-17) will be applied.

For the Level 2 PSA the HRA methodology is similar to that for the Level 1 PSA, with the following specific considerations for the severe accident conditions:

- Dependency between the Level 1 PSA and the Level 2 PSA
- Stress for operators in severe accident conditions
- The environmental effect of radiation, especially on the field operators
- Evacuation from MCR to an alternate location
- Instrument failure affecting HEPs

All the important human actions from the PSA will be captured in the HSRC database, (refer to Section 15.4.1.4 above).

Additional information on the HRA methodology can be found in the “BWRX-300 Standard Plant Probabilistic Safety Assessment Methodology” (006N2915, (Reference 15.4-21)) and “Probabilistic Safety Assessment Summary” (008N9751 (Reference 15.4-22)).

15.4.3.3 Quantification of Human Error Probabilities

For the Type A important human actions, the EPRI “HRA Calculator Software Manual,” (Reference 15.4-23) will be used to derive an HEP based on the Accident Sequence Evaluation Program method.

The Type C important human actions will be modelled as being composed of two elements, a cognitive element, and an execution/action element. The cognitive element involves the act of recognising the need to perform an action, or procedure step. It may also encompass the operations staff briefing on an evolution. Execution involves the actual tasks taken by the operator to bring the plant to a safe stable state.

The EPRI HRA Calculator uses the Cause-Based Decision Tree Method (CBDTM) and/or the Human Cognitive Reliability/Operator Reactor Experiments (HCR/ORE) methods to derive an HEP for the cognitive element of the Type C important human actions (Reference 15.4-23), see Appendix B, Forward Action PSR15.4-188). The Technique for Human Error Rate

Prediction (THERP) is then used to derive the HEP for the execution/action element of the HEP (Reference 15.4-23).

As the development of the PSA models are in their early stages, screening HEPs are currently used. The EPRI HRA Calculator approach described above has been used to derive screening HEPs for important human actions when at-power. For the low power and shut down events and spent fuel pool events PSAs, the screening HEPs have been based on engineering judgment, with suitable justification being provided.

The quantification of any HEPs associated with Type B important human actions will be undertaken on a case-by-case basis, depending on the nature of the action and error. As discussed in Section 15.4.1.2, Type B important human actions may involve errors made by personnel during planned maintenance activities, or errors made by personnel during normal operations while changing the state of equipment. The latter may also include modelling of operator actions to recover the error before it escalates into an initiating event. Therefore, the HRA Calculator will be used to apply the most appropriate human error quantification technique for the error being quantified.

The HRA Calculator will be used for Operator Action Dependency Analysis (008N9751 (Reference 15.4-22)). The analysis is performed with the HEPs set to 1.0 or a value close to 1.0 to drive the human actions higher in risk and keep them from being truncated out in the quantification by the frequency cut-off. Instances where there are multiple human actions in a single cut-set are then identified. A decision tree will be applied to consider the dependency coupling mechanisms and the potential level of dependency. The levels of dependency utilised and the treatment of the HEPs will be based on application of THERP (Reference 15.4-23). Additionally, where there is potential for common cognitive failure between important human actions this will be addressed through the modelling.

15.4.3.4 Human Failure Contribution Captured within Reliability Data

For GDA, the PIEs developed in the initiating event analysis include contributions from human error in the historical failure rates. Thus, the current initiating event analysis assumes that human error induced initiating events are already considered within the initiating event groups/categories. These events are assumed to be subsumed in the applicable event occurrence data (general transient, loss of offsite power, loss of feedwater, etc.). As discussed in Section 15.4.1.2 above, the HFEA takes a qualitative approach to identify plausible and relevant Type B human actions, which includes gaining an understanding of the underlying human error mechanism. The identification of the potential human “initiation” of these failures and hazards, ensures consideration of the human error causes, which leads to more realistic frequency estimation, and informs aspects of the design, such that error potential may be reduced. At present, no Type B human actions are included in the BWRX-300 PSA model (refer to Forward Action PSR15.4-192 in Table B-1, Appendix B).

The PSA Model contains limited component-level information for some systems because design information at the component level is still in flux at this stage of the plant design process. Generic nuclear industry component reliability data (Reference 15.4-24) has been used for the majority of components. Where appropriate, this data includes the contribution to the component reliability made by human error. Insights into the risk significance of human machine interactions that are implicit within the component reliability data are provided by the component importances presented in Appendix F of the “PSA Summary Report” (008N9751 (Reference 15.4-22)).

Regarding Safety Classification, though human actions are not explicitly assigned a Safety Classification a process is in place that ensures human actions are addressed in a proportionate manner. As stated in Section 15.4.1.1, the HFE programme takes a proportionate approach to addressing human actions within the design (“BWRX-300 HFE Program Plan” 0075N1716 (Reference 15.4-11)). This is achieved through assigning risk

levels and associated HFE application levels to tasks, categorising HSRCs, and considering the nuclear safety criteria and equipment reliability requirements associated with SSCs (in accordance with the generation capability criteria as defined within the HFE Program Plan (005N1716 (Reference 15.4-11)).

15.4.3.5 Modelling of Type A Human Actions within the PSA

The BWRX-300 PSA supporting the GDA review represents an early iteration of the analysis. At this stage in the design, a large amount of engineering judgement must also be used. As the design develops and operating procedures and examination maintenance inspection and testing schedules are produced, more detailed HRA analysis of Type A human actions is performed. Going forward, the intention is to keep assessing the Type A human actions as more information becomes available, to ensure comprehensive coverage of potential risk due to operator error (Appendix B, Forward Action PSR15.4-191).

An initial exercise to identify Type A human actions identified possible candidates based on the types of human error traditionally modelled in a PSA, i.e. mispositioning errors and miscalibration errors. However, these were mostly screened out on the basis they were not credible for the BWRX-300 design, as discussed in the following paragraphs.

Mispositioning errors arise when there is a failure to restore equipment to its standby status after testing or maintenance. Though in-service testing requirements and maintenance and surveillance procedures are not currently available, a screening was performed to determine, for each system modelled in the PSA, whether there are potential mis-positionings that could have a significant effect on system unavailability. The PSA Summary Report (008N9751 (Reference 15.4-22)) records that for all but one system either the screening rules may be applied or there are no mis-positionings that could affect the PSA model for the systems. The exception relates to System G11: Boron Injection System where failure to reopen the manual pump isolation valves could result in a mispositioning event (see basic event G11-HFE-TA-MISPOS in Table 6-43, 008N9751 (Reference 15.4-22)). This Type A human action was identified after the GDA PSA had been prepared and does not appear in the GDA PSA model.

Although operating and calibration procedures are not currently available, a screening was performed for each system modelled in the PSA to determine whether there are potential miscalibrations that could have a significant effect on system unavailability. Table 6-43 in the “PSA Summary Report” (008N9751 (Reference 15.4-22)) records several Type A human actions that were developed as a result of the system screening. However, based on subsequent discussions with design engineers and engineering judgment they were excluded from the PSA model. This was justified on the basis that the Technical Specification Monitor (TSM) performs automatic channel checks that detect miscalibration errors and promptly alert the operators to an issue. The TSM provides surveillance test support and identifies deviations from plant technical specification requirements where appropriate plant signals are available. The divisions output their measures for the relevant parameters at least once per second. The TSMs compare the outputs to each other and alarms on range checks and inconsistencies. Measures may also be compared to those from lesser SC (SC2 and SC3) systems with additional alarms for discrepancies. Therefore, instead of channel checks being performed per the typical technical specification intervals of once a week or once a day, the channel checks are performed continuously (described in 006N5114, “BWRX-300 Plant I&C Systems Architecture Requirements and Design”, (Reference 15.4-25)). Therefore, given that the TSM would identify discrepancies and alert the operator if miscalibration of components in the above systems occurred, it is judged not to be credible that a miscalibration would remain undetected. It should also be highlighted that TSM alarms and indications are designed in accordance with HFE design processes and inputs (see Chapter 18 for further information on HFE design processes).

The identification of Type A human actions resides within the PSA team in accordance with the "BWRX-300 Safety Strategy" (refer to 006N5064, Reference 15.4-13). However, the activities that are undertaken by the HFE team associated with updating the HFEA may also identify Type A human actions. If so, these should be communicated to the PSA team for screening and potential incorporation into the PSA model. Hence a forward action has been raised to capture this interfacing action (see Appendix B, Forward Action PSR15.4-360).

15.4.3.6 The Risk Significance of Human Actions in the Full Power Internal Events PSA Model

The Type A and Type C human actions developed for the BWRX300 Full Power Internal Events (FPIE) PSA model are documented in Tables 6-42 and 6-43 respectively, in the "PSA Summary Report" (008N9751 (Reference 15.4-22)). However, not all of the human actions that were developed were used when the model was compiled. No Type A human actions were included in the FPIE model and no Type B human actions were developed at the time of model integration. Several Type C human actions were considered and developed, or partially developed but later excluded. The FPIE PSA model includes several of these events, but the HEPs are set to 1.0 in the model (no credit is taken for the action), and they are either not used or used for sensitivity cases. For example, an action to undertake manual containment venting was developed, but a HEP of 1.0 has been applied. Consideration of the response time (venting needs to occur quickly) resulted in the conclusion that manual containment venting is not a credible recovery action. The design was therefore modified to include a rupture disc in the containment vent line.

Only one post-initiator human action is credited within the FPIE PSA model. This relates to the Boron Injection System. This appears in the cutsets/results (Section 6.8.1.4 of 008N9751 (Reference 15.4-22)). The PSA Summary Report (Section 6.9.1.3 of 008N9751 (Reference 15.4-22)) presents the result of a sensitivity study on this human action that utilised the 5th and 95th percentile HEP values. The results of the sensitivity study were as follows:

- Baseline CDF/year 1.06E-08
- HEP 5th percentile value 1.05E-08 difference -0.8%
- HEP 95th percentile value 1.08E-08 difference 1.9%

These results show a small increase in the CDF compared to the base Level 1 PSA model for the 95th percentile value HEP. The sensitivity with the 5th percentile value HEP show a slight decrease and negligible impact to CDF. These results show that uncertainty in human reliability has only a small impact on the BWRX-300 FPIE Level 1 PSA. These results, reflect the implementation of the BWRX-300 Safety Strategy and design philosophy to reduce the human contribution to risk.

15.4.3.7 The Risk Significance of Human Actions in the LPSD PSA Model

The human actions modelled in the Low Power and Shutdown (LPSD) Internal Events Level 1 PSA model differed slightly to those in the FPIE PSA model. The human actions modelled are presented in Tables 6-42 and 6-43 of the "PSA Summary Report" (008N9751 (Reference 15.4-22)). These include a single Type A human action that models a DL4 ICS miscalibration event. This was included due to uncertainty as to whether the function would be analog or digital.

In the LPSD Internal Events Level 1 PSA, six out of the ten human action events appear in the PSA results. The contribution from these events is not a significant source of risk as they all have low FV and RAW results and no human action events appear in the top 500 cutsets.

A human reliability sensitivity was performed to better understand the impact of operator interactions in the PSA results and to gain insight into the importance of these actions on the

LPSD Internal Events Level 1 PSA. The sensitivity studies were conducted with all HEPs set to either their 5th or 95th percentile value.

- Baseline CDF/year 1.20E-09
- HEP 5th percentile value 1.20E-09 difference -0.5%
- HEP 95th percentile value 1.22E-09 difference1.3%

These results show that uncertainty in human reliability has a small impact on the BWRX-300 LPSD Internal Events Level 1 PSA and that human actions are of low importance, as per the Safety Strategy.

15.4.4 References

15.4-1 NEDC-34190P, “BWRX-300 UK GDA Chapter 18: Human Factors Engineering,” Rev B, GE-Hitachi Nuclear Energy, Americas, LLC.

15.4-2 NEDC-34165P, “Chapter 3A: Safety Objectives and Design Rules for SSCs,” Rev B, GE-Hitachi Nuclear Energy Americas, LLC.

15.4-3 NEDC-34179P, “Chapter 15.1: General Considerations of the BWRX-300 Safety Analysis,” Rev B, GE Hitachi Nuclear Energy Americas, LLC.

15.4-4 NEDC-34183P, “BWRX-300 UK GDA Chapter 15.5: Deterministic Safety Analyses,” Rev B, GE-Hitachi Nuclear Energy, Americas, LLC.

15.4-5 NEDC-34184P, “BWRX-300 UK GDA Chapter 15.6: Probabilistic Safety Assessment,” Rev B, GE-Hitachi Nuclear Energy, Americas, LLC.

15.4-6 NEDC-34185P, “BWRX-300 UK GDA Chapter 15.7: Internal Hazards,” Rev B, GE-Hitachi Nuclear Energy, Americas, LLC.

15.4-7 NEDC-34186P, “BWRX-300 UK GDA Chapter 15.8: External Hazards,” Rev B, GE-Hitachi Nuclear Energy, Americas, LLC.

15.4-8 NEDC-34176P, “BWRX-300 UK GDA Chapter 13: Conduct of Operations,” Rev B, GE-Hitachi Nuclear Energy, Americas, LLC.

15.4-9 NEDC-34191P, “BWRX-300 UK GDA Chapter 19: Emergency Preparedness and Response,” Rev B, GE-Hitachi Nuclear Energy, Americas, LLC.

15.4-10 NEDC-34199P, “BWRX-300 UK GDA Chapter 27: ALARP Evaluation,” Rev B, GE-Hitachi Nuclear Energy Americas, LLC.

15.4-11 005N1716, “BWRX-300 Human Factors Engineering Program Plan,” GE-Hitachi Nuclear Energy Americas, LLC.

15.4-12 005N3747, "Human Factors Engineering Concept of Operation for BWRX-300, " Rev 1, GE-Hitachi Nuclear Energy Americas, LLC, 2024.

15.4-13 006N5064, “BWRX-300 Safety Strategy,” GE-Hitachi Nuclear Energy Americas, LLC.

15.4-14 007N3073, “BWRX-300 Human Operation Hazard Evaluation,” Rev 0, GE-Hitachi Nuclear Energy Americas, LLC, 2024.

15.4-15 007N3447, “Human Factors Engineering Safety Analysis,” Rev 0, GE Hitachi Nuclear Energy Americas, LLC, 2024

15.4-16 005N3558, “BWRX-300 Fault Evaluation and Fault List,”” GE-Hitachi Nuclear Energy Americas, LLC.

15.4-17 RA-S-1.1-2022, “Standard for Level 1 - Large Early Release Probabilistic Risk Assessment for Nuclear Power Plants,” American Society of Mechanical Engineers, 2022.

15.4-18 IAEA-TECDOC-1804, “Attributes of Full Scope Level 1 Probabilistic Safety Assessment (PSA) for Applications in Nuclear Power Plants,” International Atomic Energy Agency, 2016.

15.4-19 ONR NS-TAST-GD-063, “Technical Assessment Guide Human Reliability Analysis,” Office for Nuclear Regulation, 2022.

15.4-20 EPRI NP-3583, “Systematic Human Action Reliability Procedure (SHARP), Electric Power Research Institute,” Electric Power Research Institute, 1984.

15.4-21 006N2915, “BWRX-300 Standard Plant Probabilistic Safety Assessment Methodology,” GE-Hitachi Nuclear Energy Americas, LLC.

15.4-22 008N9751, “BWRX-300 Probabilistic Safety Assessment Summary Report for UK Generic Design Assessment (GDA) Review,” GE-Hitachi Nuclear Energy Americas, LLC.

15.4-23 EPRI 3002010680, “The HRA Calculator Software Manual,” Electric Power Research Institute, 2017.

15.4-24 NUREG/CR 6928, “Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants”, U.S. Nuclear Regulatory Commission Office of Nuclear Regulatory Research, 2007.

15.4-25 006N5114, “BWRX-300 Instrumentation and Control Architecture Design Description”, Rev 1, GE-Hitachi Nuclear Energy Americas, LLC.

15.4-26 “Safety Assessment Principles for Nuclear Facilities,” Office for Nuclear Regulation.

15.4-27 NEDC-34140P, “BWRX-300 Safety Case Development Strategy,” GE-Hitachi Nuclear Energy Americas, LLC.

APPENDIX A CLAIMS, ARGUMENTS, AND EVIDENCE

A.1 Claims, Arguments and Evidence

The ONR SAPs 2014, "Safety Assessment Principles for Nuclear Facilities," (Reference 15.4-26) identify the expectation of the ONR n that a safety case should clearly set out the trail from safety claims, through arguments to evidence. The Claims, Arguments and Evidence (CAE) approach is explained as follows:

- Claims (assertions) are statements that indicate why a facility is safe
- Arguments (reasoning) explain the approaches to satisfying the claims
- Evidence (facts) supports and forms the basis (justification) of the arguments

The GDA CAE structure is defined within NEDC-34140P, "BWRX-300 Safety Case Development Strategy," (SCDS) (Reference 15.4-27) and is a logical breakdown of an overall claim that:

> *"The BWRX-300 is capable of being constructed, operated and decommissioned in accordance with the standards of environmental, safety, security and safeguard protection required in the UK."*

This overall claim is broken down into Level 1 claims relating to environment, safety, security, and safeguards, which are then broken down again into Level 2 area related sub-claims and then finally into Level 3 (chapter level) sub-claims.

The Level 3 sub-claim identified within the SCDS (Reference 15.4-27) that this subchapter demonstrates compliance against is as follows:

2.3.5 Human Factors assessments have been integrated into the design, safety assessments and management arrangements, to meet the relevant safety requirements.

Important human actions are a subset of the HMIs addressed by human factors that relate to nuclear safety. As such, the treatment of important human actions also contributes to the demonstration of compliance for other chapter level sub-claims (Table A-1).

This PSR subchapter has derived a suite of arguments that summarise how the applicable Level 3 sub-claims are met (Table A-1).

It is not the intention to generate a comprehensive suite of evidence to support the derived arguments, as this is beyond the scope of GDA Step 2. However, where evidence sources are available, examples are provided in the section of the Subchapter referenced in Table A-1.

A.2 Risk Reduction As Low As Reasonably Practicable

It is important to note that nuclear safety risks cannot be demonstrated to have been reduced ALARP within the scope of a 2-Step GDA. In relation to important human actions, understanding the human contribution to risk and achieving an ALARP position requires information that is not available at GDA Step 2 such as the full suite of tasks to be performed (tasks claimed in the safety studies and other important human actions, for example relating to maintenance and refuelling), as well as details on conduct of operations. It is considered that the most that can be realistically achieved is to provide a reasoned justification that the BWRX-300 design aspects will effectively contribute to the development of a future ALARP statement. In this respect, this subchapter contributes to the overall future ALARP case by demonstrating that the subchapter-specific arguments derived may be supported by existing and future planned evidence for the arguments in Table A-1.

Probabilistic safety aspects of the ALARP argument are addressed within PSR Subchapter 15.6 - Probabilistic Safety Assessment.

Table A-1: Human Actions and Related Claims and Arguments

Subchapter 15.4 Claim	Subchapter 15.4 Argument	Sections and/or Reports that Evidence the Arguments
2.1 All functions have been derived and substantiated taking into account RGP and OPEX, and processes are in place to maintain these through-life.		
2.1.2 The design of the system has been substantiated to achieve the safety functions in all relevant operating modes.	HEA contributes to design substantiation by confirming that important human actions that support safety functions are feasible and can be reliably performed.	15.4.1.5 Substantiation of Claims on Important Human Actions through Qualitative HEA
	The HFE V&V program evaluates the plant design (in parts and as an integrated whole) against safety case requirements, HFE design principles and requirements, user task requirements, job design and staff complement, procedural accuracy and usability, and effectiveness of training. In addition, HFE V&V activities provide the evidence that supports the substantiation of important human actions credited within the DSA and PSA.	15.4.1 General Considerations (in particular HFE V&V) 15.4.1.5 Substantiation of Claims on Important Human Actions through Qualitative HEA 15.4.2.9 Substantiation of Human Actions Claimed in the DSA
2.3 A suitable and sufficient safety analysis has been undertaken which presents a comprehensive fault and hazard analysis that specifies the requirements on the safety measures and informs emergency arrangements (Safety Analysis)		
2.3.5 Human Factors assessments have been appropriately integrated into the design, safety assessments and management arrangements, to meet the relevant safety requirements.	A graded (or proportionate) approach is applied to the conduct of activities within the HFE Program. This provides an appropriate level of analysis to substantiate important human actions.	15.4.1.1 Proportionate/Graded Approach 15.4.1.4 Human Safety and Reliability Claims Database 15.4.1.5 Substantiation of Claims on Important Human Actions through Qualitative HEA

Subchapter 15.4 Claim	Subchapter 15.4 Argument	Sections and/or Reports that Evidence the Arguments
	The results from the HEA, including human factors issues, assumptions and requirements feed into the design and the development of organisational arrangements such as staffing, training, and procedures.	15.4.1.4 Human Safety and Reliability Claims Database
	Risk-proportionate task analysis is carried out to analyse tasks allocated to human or shared during the Allocation of Function process. The overall objective is to identify design requirements to ensure that tasks, including any important human actions claimed in the BWRX-300 safety analyses, are feasible and can be reliably performed.	15.4.1 General Considerations
2.4 Safety risks have been reduced as low as reasonably practicable		
2.4.1 RGP has been taken into account across all disciplines.	The elements of the HFE program and methodologies relating to important human actions are based on international standards, guidance, RGP and multiple nuclear regulatory requirements.	15.4.1 General Considerations
2.4.2 Operating Experience (OE) and Learning from Experience (LfE) has been taken into account across all disciplines.	The HFE program includes the identification, review, use and application of Operating Experience to ensure that HF issues (lessons learned and good practice) are incorporated into the design and safety analyses.	15.4.1 General Considerations

APPENDIX B FORWARD ACTION PLAN

Table B-1: Human Actions: Forward Actions

Action ID	Finding	Forward Actions	Delivery Phase
PSR15.4-185	In defining a proportionate approach to substantiation of human actions, only FV has been identified as a measure of risk significance for Category 2 HSRCs in the Human Factors Engineering Safety Analysis methodology (007N3447, Revision 0). It would be usual to use additional measures e.g., Risk Increase Factor (RIF)/Risk Achievement Worth (RAW) or consider the sensitivity to a shift in HEP of a number of orders of magnitude.	The approach to determining the risk significance of Category 2 Human Safety and Reliability Claims (HSRCs) within the HFE Safety Analysis Methodology (Revision 0) should include measures of risk significance that consider the sensitivity of the total risk to each of the HEPs that are used i.e. RAW.	For PCSR/PCER
PSR15.4-186	ONR's position is that no human error quantification methods have been fully validated for modelling human-computer interaction.	The approach to quantification of any HEPs associated with software-based HMIs should be reviewed and justified.	Before Site License Application, Environmental Permit Applications and/or BL3 Design Phase
PSR15.4-188	The EPRI HRA Calculator uses time-reliability curves to quantify the cognitive element of human actions. THERP is used for the execution element. ONR have concerns over the use of time-reliability curves, especially where they are used to screen human actions.	Methodologies for analysing human actions to be revised to explain and justify the use of the cognitive models within the EPRI HRA Calculator in relation to screening and task analysis.	For PSCR/PCER
PSR15.4-189	Violations in general are not within GEH's scope for Step 2. However, ONR's expectation is that consideration should be given to the potential for design induced violations, e.g., where plant layout or task design may result in the operator perceiving inefficiencies that they subsequently work around.	The task analysis methodology and approach to HFE V&V should be revised to give consideration to the potential for design induced violations, for instance, whether task design is inefficient, such that operators could be motivated to seek more efficient ways of completing tasks. This will be required before	For PCSR/PCER

Action ID	Finding	Forward Actions	Delivery Phase
		site-specific V&V studies are undertaken (see PSR18-180).	
PSR15.4-191	The majority of the Type A Human Actions: Pre-Initiating Event (Type A) Human Actions are not currently modelled in the PSA due to the incomplete design of the plant.	Some Type A events have already been identified (e.g. miscalibration errors) and screened out from the PSA model as explained within the GDA Step 2 PSA Summary Report (008N9751 Revision 1). Further analysis will be conducted to identify, screen and model Type As as the design evolves and procedures are developed.	For PCSR/PCER
PSR15.4-192	Type B Human Actions: Currently no Initiating Events Induced by Human Actions (Type B events) have been identified in the PSA.	Further analysis will be conducted by HFE in accordance with the Human Failure Events Analysis methodology (next revision from Revision 0 of 007N3073) as the design evolves and procedures are developed to identify Type B events for consideration in the safety analysis.	For PCSR/PCER
PSR15.4-360	Identification of Type As resides within the PSA team in accordance with the BWRX-300 Safety Strategy (006N5064). However, the activities that are undertaken by HFE as part of the updated HOHE methodology (post GDA referred to as the Human Failure Event Analysis) may identify Type As which would be useful to provide to the PSA for screening and potential incorporation into the PSA model.	Update the Safety Strategy (006N5064, Revision 6) to include the Human Failure Events Analysis (HFEA) work led by HFE and qualitative HRA, as a mechanism to identify and screen pre-initiator Type A HFEs. This will enable outputs from the HFEA to be used by PSA in the identification, screening and modelling of pre-initiator Type As within the PSA model.	For PCSR/PCER
PSR15.4-361	Operator actions reflected in the BL-DSA as DL1 provisions are not explicitly identified within the Fault Evaluation (005N3558, Revision 3). Accordingly, for GDA	Incorporate operator actions reflected in the BL-DSA as DL1 provisions (following	For PCSR/PCER

Action ID	Finding	Forward Actions	Delivery Phase
	Step 2, the HSRC Register does not include DL1 Baseline Human Actions.	revisions to the Fault Evaluation (005N3558)) in the following documentation: - An updated version of the safety case - The HSRC register following the explicit identification of BL1 DL actions within the Fault Evaluation (005N3558)	
PSR15.4-362	Operator actions reflected in the BL-DSA as DL1 provisions are not explicitly considered within the following HFE methods: • Determining the HFE application level (HFE Program Plan 005N1716 Revision 2 and HFE AoF Methodology 006N4192 Revision 1). The nuclear safety criterion only includes credited DSA and PSA actions • Assigning an HSRC to a claim category (Table 3-1 of 007N3447 HFE Safety Analysis Methodology). The categories include credited DSA actions and modelled PSA actions but not DL1 Baseline Actions	Update the nuclear safety criterion ((HFE Program Plan 005N1716 Revision 2 and HFE AoF Methodology 006N4192 Revision 1) that is used to determine the HFE application level to include operator actions reflected in the BL-DSA as DL1 provisions. Update the HSRC Category Table (Table 3-1 of the HFE Safety Analysis Methodology 007N3447) to include operator actions reflected in the BL-DSA as DL1 provisions.	For PCSR/PCER