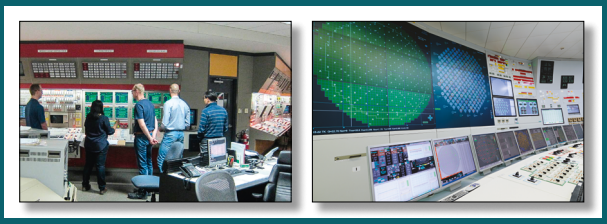
Human Aspects of Nuclear Safety
2019

Multi-Stage Validation of Nuclear Power Plant Control Room Designs and Modifications



OECD
BETTER POLICIES FOR BETTER LIVES

NEA
NUCLEAR ENERGY AGENCY

Human Aspects of Nuclear Safety

Multi-Stage Validation of Nuclear Power Plant Control Room Designs and Modifications

© OECD 2019
NEA No. 7466

NUCLEAR ENERGY AGENCY
ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

The OECD is a unique forum where the governments of 36 democracies work together to address the economic, social and environmental challenges of globalisation. The OECD is also at the forefront of efforts to understand and to help governments respond to new developments and concerns, such as corporate governance, the information economy and the challenges of an ageing population. The Organisation provides a setting where governments can compare policy experiences, seek answers to common problems, identify good practice and work to co-ordinate domestic and international policies.

The OECD member countries are: Australia, Austria, Belgium, Canada, Chile, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Israel, Italy, Japan, Korea, Latvia, Lithuania, Luxembourg, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, the Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The European Commission takes part in the work of the OECD.

OECD Publishing disseminates widely the results of the Organisation's statistics gathering and research on economic, social and environmental issues, as well as the conventions, guidelines and standards agreed by its members.

This work is published on the responsibility of the OECD Secretary-General.

NUCLEAR ENERGY AGENCY

The OECD Nuclear Energy Agency (NEA) was established on 1 February 1958. Current NEA membership consists of 33 countries: Argentina, Australia, Austria, Belgium, Canada, the Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Korea, Luxembourg, Mexico, the Netherlands, Norway, Poland, Portugal, Romania, Russia, the Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The European Commission and the International Atomic Energy Agency also take part in the work of the Agency.

The mission of the NEA is:

- to assist its member countries in maintaining and further developing, through international co-operation, the scientific, technological and legal bases required for a safe, environmentally friendly and economical use of nuclear energy for peaceful purposes;
- to provide authoritative assessments and to forge common understandings on key issues, as input to government decisions on nuclear energy policy and to broader OECD policy analyses in areas such as energy and sustainable development.

Specific areas of competence of the NEA include the safety and regulation of nuclear activities, radioactive waste management and decommissioning, radiological protection, nuclear science, economic and technical analyses of the nuclear fuel cycle, nuclear law and liability, and public information. The NEA Data Bank provides nuclear data and computer program services for participating countries.

This document, as well as any data and map included herein, are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

Corrigenda to OECD publications may be found online at: *www.oecd.org/about/publishing/corrigenda.htm*.

© OECD 2019

You can copy, download or print OECD content for your own use, and you can include excerpts from OECD publications, databases and multimedia products in your own documents, presentations, blogs, websites and teaching materials, provided that suitable acknowledgement of the OECD as source and copyright owner is given. All requests for public or commercial use and translation rights should be submitted to *neapub@oecd-nea.org*. Requests for permission to photocopy portions of this material for public or commercial use shall be addressed directly to the Copyright Clearance Center (CCC) at *info@copyright.com* or the Centre français d'exploitation du droit de copie (CFC) *contact@cfcopies.com*.

Cover photos: Inspection of control room, Darlington, Canada (CNSC); Central control room of nuclear power plant (Shutterstock, Nordroden).

Foreword

Integration of the experts' workshop results

In 2015, the Nuclear Energy Agency (NEA) brought together leading nuclear sector experts in nuclear power plant control room validation to participate in the Experts' Workshop on Human Factors Validation of Nuclear Power Plant Control Room Designs and Modifications. The theme and focus of the 2015 workshop was on identifying means for achieving reasonable confidence in validation results and conclusions. Many of the participating experts identified multi-stage validation (MSV) as among the most promising pathways towards establishing reasonable confidence. However, it was noted at the time that the MSV concept had not been formally defined and implementation guidance was limited. As a result, the NEA initiated a programme of work to explore the potential of MSV. The NEA Working Group on Human and Organisational Factors (WGHOF), under the auspices of the NEA Committee on the Safety of Nuclear Installations (CSNI), developed the present report to serve as a common basis for future efforts to discuss and develop research, guidelines, regulatory practices and strategies concerning MSV.

Work on this report was conducted in three phases. Initial development of the report was completed as a collaborative effort of a nine-member task group. The task group comprised human factors professionals from a variety of sectors within the nuclear power industry, including regulatory authorities, national laboratories, utilities, nuclear plant vendors and independent consultants. In the second phase, the draft report was issued to a similarly diverse group of 12 independent experts for review. These experts then convened with the task group for a 3-day workshop between 8-10 June 2018, in San Francisco, California. The general format of the workshop consisted of presentations on specific elements of the draft report, followed by commentary presentations by each of the independent experts, and then a period of general dialogue, followed by breakout sessions that allowed more in-depth and focused discussions among independent experts and members of the task group.

Biographical sketches of workshop participants and the detailed agenda for the workshop are provided in Appendices A and B, respectively. In the third phase of development for this report, the feedback and insights gained through the workshop were compiled and reviewed by the task group. These comments were dispositioned through a series of task group meetings using a consensus approach. The draft report was revised to reflect these comment resolutions.

Among the many comments and insights gained through the workshop, three were particularly substantive in their impact on the thinking of the task group and consequently the characterisation of MSV as presented in this report. The focus of these comments was on:

- the characterisation of MSV as a process that occurs throughout the entire life cycle of a system;
- the aggregation of data across stages of an MSV;
- the integration of MSV results, and presentation of the case for validation.

The task group came to an early consensus in the development of the draft report that MSV was a process that spanned the entire life cycle of a system. This view was reflected in an example showing validation activities at various design stages, beginning with *planning and analysis* and *requirements specification* as the first two stages, as well as *deployment and operations* as the final stage. Through the workshop, task group members were made aware that while there did not appear to be a general concern with the life-cycle view from a conceptual perspective, there were practical concerns. For example, some of the independent experts questioned conducting validation activities at the *Planning and Analysis* stage as they did not see sufficient benefit given the perceived limitations of the methods, applicability of the results to the final design, or the time/labour costs of the activities. There were also concerns expressed about the types of activities that could be performed at these early stages, which were perhaps better characterised as verification rather than validation activities. By contrast, most experts did not question conducting validation activities once conceptual designs had been developed. In response to this feedback, the report was revised to eliminate the *Planning and Analysis* and *Requirements Specification* stages from the MSV example presented in Chapter 4. Although MSV as described in this report would not exclude or preclude such activities, the task group determined that a more focused example was preferable for a report addressing the basic concept of MSV.

Also related to the life-cycle view of MSV were concerns from some of the experts regarding validation at the *deployment and operations* stage. Here, the concern was more based on the view that validation during a design process has different characteristics than validation following operational experience. According to this view, validation prior to operation is closely linked to a decision (e.g. by the regulatory body or the utility) that a system can be placed in operation and under what conditions. A view that validation continues through deployment and operations has the potential to cause ambiguity or confusion with regard to when a system has been "validated." Despite such concerns, there was general agreement that applying a validation perspective to the monitoring and evaluation of operating experience during deployment and operations was achievable and could be of value. Weighing these views, the task group in the end elected to retain *deployment and operations* as an example of a design stage included in MSV.

In the initial conception of MSV (i.e. the pre-workshop paper) the task group set forth three defining characteristics of MSV, with the third characteristic being:

> Individual validation activities are conducted and grouped in time, as stages, that allow meaningful aggregation, summation or comparison of data, both within and across stages, so as to support interim or final validation conclusions.

During the workshop, independent experts were invited to comment on each of the defining and desirable characteristics. Whereas comments on other characteristics were largely aimed towards gaining clarity, technical concerns were raised regarding this third defining characteristic of MSV. More specifically, the experts questioned whether aggregating data across stages was feasible in a manner that was technically sound. Through discussion at the workshop, and subsequently among the task group members, it was concluded that aggregation or comparison across stages at the raw *data* level was not likely to be meaningful, and that the *results* (e.g. conclusions) obtained at each stage were the more appropriate unit of analysis. As a result, the third defining characteristic and associated text were revised accordingly.

As noted above, the third area where substantive feedback from the independent experts was received concerned the preliminary report's treatment of how results obtained through MSV were integrated, and a case made for the validation of a system. The experts, in general, did not see that these concepts were sufficiently well developed. This criticism was, by and large, expected as it was consistent with the self-assessment of the efforts to that point. Fortunately, discussions during and following the workshop led to the identification of a promising model for integrating results from multiple validation tests and structuring a case for validation. Discussion of this model is incorporated in Chapter 5 of this report.

Acknowledgements

This report was developed by a task group of the Nuclear Energy Agency (NEA) Working Group on Human and Organisational Factors (WGHOF). The task group comprised the following individuals: Per Øivind Braarud (Halden Reactor Project); Cecilia De la Garza (Électricité de France); David Desaulniers, Task Lead (US Nuclear Regulatory Commission [NRC]); Stephen Fleger, (NRC); Paula Savioja-Kangasluoma (Radiation and Nuclear Safety Authority, Sweden); Jari Laarni (VTT Technical Research Centre of Finland); Dina Notte (ERGODIN); John O'Hara (Brookhaven National Laboratory, United States) and Cyril Rivere, Areva. The NRC served as the lead organisation.

In addition, the task group was fortunate to have the support of a panel of experts who donated their time to critique the initial draft of this report and freely shared their expertise as workshop participants. The members of the expert panel were: Joakim Bergroth (Fortum); Maren H.R. Eitrheim (Institute for Energy Technology, Norway); Robert Fuld (Westinghouse Electric Company); Brian Green (NRC); Conny O. Holmstrom (Vatenfall AB); Hanna Koskinen (VTT), Wolfgang Krause (Areva GmbH); Robert Leger (Candu Energy Incorporated, Canada); Nathan Lau (Virginia Polytechnic Institute and State University); Luis Rejas Lopez (Tecnatom SA); Kenji Mashio (Mitsubishi Heavy Industries); and Alice Salway (Canadian Nuclear Safety Commission [CNSC]).[1] Logistical support for the experts' workshop was provided by Aaron Derouin, CNSC; Radim Dolezal (State Office of Nuclear Safety, Czech Republic); Monica Haage (formerly of the NEA) and Niav Hughes (NRC).

The NEA WGHOF extends its appreciation to all of these individuals and their organisations for their generosity in contributing their time and expertise to this effort.

1. See Appendix A for biographical sketches of the members of the WGHOF task group on multi-stage validation and of expert panel members.

Table of contents

List of abbreviations and acronyms

CSNI	Committee on the Safety of Nuclear Installations (NEA)
HED	Human engineering discrepancy
HFE	Human factors engineering
HMI	Human-machine interface
HSI	Human-system interface
IAEA	International Atomic Energy Agency
IEEE	Institute of Electrical and Electronics Engineers
ISV	Integrated system validation
ISO	International Organization for Standardization
IEC	International Electrotechnical Commission
MCR	Main control room
MSV	Multi-stage validation
NEA	Nuclear Energy Agency
NPP	Nuclear power plant
NRC	Nuclear Regulatory Commission (United States)
OECD	Organisation for Economic Co-operation and Development
PV	Preliminary validation
SUC	Systems usability case
US-APWR	US Advanced Pressurised Water Reactor
V&V	Verification and validation
VTT	VTT Technical Research Centre of Finland Ltd.
WGHOF	Working Group on Human and Organisational Factors (NEA)

Executive summary

The human factors engineering (HFE) validation of a nuclear power plant (NPP) control room design is a complex undertaking with many technical and logistical challenges. Validations must address the diversity of operating conditions, staffing configurations and failure scenarios that the plant may experience or is designed to tolerate, and yet these validations must be conducted within the practical constraints of available resources. How these challenges are addressed can impact the confidence that vendors, nuclear plant operating companies and regulatory authorities have in the validation results and conclusions.

This report proposes a specific approach, referred to as multi-stage validation (MSV), for validating systems through a series of successive, co-ordinated activities performed at multiple points or periods during the development or modification of a control room design. A mature and well-guided MSV approach has the potential to reduce risk in the design process, increase effectiveness and efficiencies in the validation process, and increase overall confidence in the results by providing opportunities to:

- address issues in a timely and cost-effective manner since they can be identified early in the design process;
- conduct a thorough validation since individual control room subsystems can be validated under controlled and focused test conditions;
- use a larger number of scenarios and a broad range of tasks and conditions over the course of the design development;
- enable longitudinal comparisons of subsystems as the design of the subsystems matures through successive modifications;
- improve validation methods through the experience gained in early, successive validations, thus reducing the risk of methodological challenges or shortcomings during the validation of the integrated system.

The scope of an MSV application described in this report covers both new, NPP main control room designs, and modifications (e.g. for modernisation) to existing NPP main control room designs. The objective of this report is to provide a common reference for future dialogue, research and development concerning MSV as an approach to validating control room designs and modifications for supporting the safe operation of NPPs.

It should be noted that MSV is a relatively new concept that has yet to be formally defined in the technical literature or in standards and guidelines on control room validation. Although some general guidance to conduct validations at multiple points in the design process is available in the literature, more specific guidance regarding matters such as how to scope, conduct and co-ordinate these validations is needed to support industry and regulatory efforts towards improving the validation process and having greater confidence in the results. To that end, this report describes three defining characteristics of MSV as follows:

1. An MSV is conducted as a series of validation activities, each with its own objective(s), method(s) and result(s).
2. Each validation activity included within an MSV is designed to provide information that can be used as part of the basis for determining whether a system can accomplish its intended use, goals and objectives in a specified environment.
3. Individual validation activities are conducted and grouped in time as stages that allow meaningful aggregation, summation or comparison of results, both within and across stages, to support interim or final validation conclusions.

Staged validation efforts should also possess certain characteristics to support the achievement of reasonable confidence in the validation results and conclusions. These "desirable characteristics" of MSV are:

1. Validations are conducted from early (conceptual) to detailed (operational) stages of design development and operations.
2. The subjects of validation comprising an MSV include design concepts (e.g. operations, automation), system elements (e.g. subsystem designs) and the integrated design, and should generally progress from system concepts and elements to the interactions and interrelationships of these elements as a sociotechnical system.
3. Results from each validation stage contribute to an accumulated body of evidence for validation of the final design.
4. Design changes made subsequent to a stage of validation are addressed through testing in the subsequent stage(s) of validation unless performance/safety is shown to be insensitive to the change or is bounded by the prior testing.
5. At each stage, validation methods, controls and rigour are commensurate with the intended use of the associated results and findings.
6. Validation testing of design elements that are novel, complex, or critical to safety is initiated early in the design process and confirmed in integrated testing.

To illustrate the MSV concept, this report provides an example of how an MSV approach could be applied during the life cycle of a design. It describes validation activities that can be conducted at the different stages of design development, including: 1) concept design; 2) subsystem design; 3) integrated system design; and 4) deployment and operations.

Properly documenting an MSV is important so as to fully derive the benefits with respect to increasing assurance of validation outcomes (i.e. confidence not only within the design team but also among other stakeholders, such as operating companies and regulators). Accordingly, this report proposes the development of an MSV portfolio to reflect the basis and breadth of validation activities conducted.

A mature and well-guided MSV is an approach that can support achieving reasonable confidence in validation results and conclusions. However, at this point in the evolution of MSV as an approach to the validation of integrated systems (e.g. limited implementation guidance and experience), there will be challenges to its effective and efficient implementation. These challenges include: 1) optimising the boundary between design and validation; 2) maintaining the boundary between design and validation; and 3) integrating MSV results. Looking towards the future, the challenges of designing and licensing the new control room designs and concepts for operations may act as potential drivers for increased use and development of MSV approaches. To support the continued maturation of MSV, areas of emphasis for future technical exchanges and guidance development could include: 1) the portfolio concept for presenting the case for validation; and 2) best practices for reducing the burden of integrated system validations through the application of MSV.

Chapter 1. Introduction

1.1. Scope, relevance and objective

This report describes a general approach and rationale for validating systems through a series of successive, co-ordinated validation activities, referred to in this report as multi-stage validation (MSV). MSV can be applied over the course of control room design development, beginning as early as concept design, and thus incorporate integrated system validation (ISV) activities in a more longitudinal approach to validation. The scope of application of the MSV addressed in this report includes human factors engineering (HFE) aspects of nuclear power plant (NPP) main control room designs, and modifications to existing NPP main control room designs.[2] MSV as described in this report, and more generally HFE validation, are thus activities conducted within the broader framework of the engineering validation of a system. This report also addresses the potential benefits of MSV, which include a better final design and increased confidence in the validation of the design. The objective of this report is to provide the nuclear power industry with a common reference for future dialogue, research and development concerning MSV as an approach to validating control room designs and modifications in support of the safe operation of nuclear power plants.

1.2. Background

Multi-stage human factors validation is a relatively new concept that has yet to be formally defined in the technical literature or in consensus standards or guideline documents on control room validation. At a conceptual level, MSV refers to the general notion of successive, co-ordinated validation efforts performed at multiple points/periods during the development of a control room design or design modification. Staged approaches to validation are referred to in different ways in the literature, for example "incremental validation" (Davey, 2004), "phased

2. As a general approach, it may be possible and perhaps desirable to apply MSV to systems (e.g. local control stations) and activities (e.g. maintenance) outside, or other than, NPP main control rooms. Consideration of such applications is beyond the scope of the project authorisation under which this report was developed. The omission of such applications is therefore solely a matter related to the scope of the effort undertaken by the Nuclear Energy Agency (NEA) Working Group on Human and Organisational Factors (WGHOF) and should not be interpreted as an implied limitation on the application of MSV.

validation" (Shin et al., 2006), "stepwise validation" (e.g. Rivere, 2015), and "multi-stage" (e.g. Laarni et al., 2017). In this report, it was elected to use the term MSV.

The potential benefits of MSV include a better final design, increased confidence in the validation of the design and a more efficient integrated system validation of the design. Many of the individuals who participated in the 2015 Nuclear Energy Agency (NEA) Experts' Workshop on Human Factors Validation of Nuclear Power Plant Control Room Designs and Modifications (see NEA, 2017) – organised by the NEA Committee on the Safety of Nuclear Installations (CSNI) – held similar views in this regard. In addition, although the specific term is not used, MSV approaches are nevertheless recommended in International Organization for Standardization (ISO) 11064 and International Electrotechnical Commission (IEC) 60964 and 61771, as well as a via regulatory guidelines (Green and Collier, 1999).

Although some guidance is available, for example, the four references cited above, this guidance provides limited detail regarding important matters of implementation and more specific guidance is needed. Experience is also limited, even if some NPP main control room (MCR) validation efforts have used an MSV approach. The industry currently lacks a common understanding of the critical elements of MSV, and how it can be conducted and documented so as to yield a stronger and/or more efficient approach to validation than is currently achieved through ISV alone. Further defining and developing the concept of MSV can support industry and regulatory efforts towards improving the validation process, while providing greater confidence in the validation results. Towards that end, the NEA/CSNI Working Group on Human and Organisational Factors (WGHOF) formed a task group to set forth a fundamental conceptualisation of MSV so as to improve awareness of its potential benefits and methods. The intent is to spur dialogue and further efforts among practitioners, researchers and regulatory authorities regarding the merits and methods by which an MSV can best be achieved.

1.3. Overview

Chapter 2 describes previous applications and descriptions of MSV approaches, emphasising the terminology used to describe these efforts and concluding with discussions on the distinction between stepwise validation and MSV, as well as the relationship between MSV and iterative design. Chapter 3 describes a proposed general conception for MSV in terms of its defining characteristics and briefly discusses several desirable characteristics for an MSV to be most effective. Chapter 4 illustrates the MSV concept by way of example and includes descriptions of potential validation activities at each stage. Chapter 5 describes an approach to aggregating the results and drawing conclusions from an MSV, and Chapter 6 addresses potential contents and attributes of the cumulative analysis that would serve as documentation of an MSV. Chapters 7 and 8 provide the task groups' conclusions regarding MSV and recommendations for future directions. References are listed at the end of the report. Appendix A provides the workshop participants and a brief summary of the relevant professional experience of each participant. Appendix B presents the agenda for each day of the three-day experts' workshop, which provided important input into the development of this report.

Chapter 2. Multi-step validation applications and terminology

As noted in a review by O'Hara and Higgins (2015), several case studies of multi-step validations are available in the technical literature (e.g. Malcolm et al., 2000; Berntson et al., 2004; Shin et al., 2006; Hanada et al., 2010; and Laarni et al., 2013). Although authors have used different terms to describe approaches to validation, such as multi-stage, stepwise, incremental and phased validation, each validation team has nonetheless implemented a multi-part, sequential approach to validation. The following summaries are organised according to the terms the authors used to describe the validation methods. The objective is to highlight where the same term has been used to describe fundamentally different concepts, and therefore where future communications regarding multi-step validations may be challenged by differing uses of key terms. An equally important objective is to highlight the different conceptions of the individual parts that can comprise a multi-step approach to validation, regardless of whether they are called steps, stages or phases, so that they can be considered relative to the conception of the multi-stage validation that is set forth in Chapter 3 of this report. More specifically, it should be noted that the validation case studies described in this Chapter are not necessarily representative examples of the multi-stage validation (MSV) concept developed later in the present report.

2.1. Example multi-step validations and terminology

Step-wise validation – Bernston et al. (2004) describe a three-part human factors validation of a secondary control area comprising a table-top validation to identify early design issues, a table-top procedure walkthrough to ensure that procedures and equipment would function together, and a full-operational trial using the final design and procedures. The authors refer to these validations as being performed in a "step-wise" fashion.

Phased validation – Hanada et al. (2010) describe the process of designing and validating the main control room (MCR) design for the US Advanced Pressurised Water Reactor (APWR); a design based on a Japanese PWR. The validation is described as being conducted in "phases". Phase 1a involved the development of the US basic human-system interface (HSI) design and testing focused only on the MCR HSI. In phase 1b, the verification and validation (V&V) continued using the same testing and analysis methods, tools and experts as those used in phase 1a. Phase 1b test scenarios focused on testing those parts of the main control room not tested in phase 1a and on exercising the changes to the design based on human engineering discrepancies (HEDs) resulting from phase1a. The results from the phase 1b testing were entered

into the HED database and assessed by an expert panel, with the end objective of refining the US basic HSI system. The objectives of phase 2 were to develop, then verify and validate through additional static and dynamic testing, the HSI inventory for the generic US-APWR. Hanada et al. (2010) describe phase 3 as identifying and making final changes to that inventory and the HSI, which may be required for a site-specific application, and ultimately to perform a final site-specific validation. At this point, the design process assumes that minimal site-specific changes will be needed in early plants and that the phase 3 testing effort will therefore be limited.

Staged validation – Malcolm et al. (2000) describe the validation of a nuclear power plant shutdown system, noting that the programme plan included formal human factors engineering (HFE) verification and validation, the largest and most extensive validation effort completed to date in the Canadian nuclear industry. This validation was completed in "stages". A preliminary walkthrough of the shutdown system changes was conducted with a group of nuclear operators using a static mock-up, to ensure that any major operational concerns were identified well before the end of the design process. The V&V stage culminated with operational trials in the full-scale control room training simulator. The simulator-based operational trials were undertaken in order to ensure that overall human-system performance requirements and expectations were achieved.

Shin et al. (2006) also describe a staged validation process. Their paper examines human factors verification and validation for the Korea Hydro Nuclear Plant Company's APR1400 computerised control room. The process, summarised in Table 2.1, is conducted in three stages spanning development to construction.

Each stage comprises the activities of suitability verification and preliminary validation, with stages 2 and 3 including multiple instances of these activities. Following a series of two preliminary validation and suitability verifications, stage 3 concludes with a "Final HFE V&V". The authors describe the process as several iterations of human factors analyses and evaluations along with design activities from small scale proof of concept tests to large-scale integrated system tests. They describe the approach as allowing management of project risks associated with new design features as a result of problems becoming evident after early stages. The approach allowed more time for handling such problems and improved confidence in the selected HSI features. The authors believe that it allowed continuous improvement, not only of the HSI features by identifying and resolving HEDs, but also of the HFE evaluation process and associated test bed. They claim that the iterative design evaluation process also allowed them to demonstrate the MCR design and its acceptability to other project stakeholders, including the regulator, and eventually to validate the advanced control room in a convergent way.

More recently Laarni et al. (2017) have made a case for the *multi-stage* approach to validation. They note that the MSV is consistent with continuous engineering approaches and describe it as "a continuous and phased/multi-staged verification and validation of nuclear power plant (NPP) control room systems." Laarni et al. (2017) identify the key characteristics of their multi-stage approach as: 1) an emphasis on a life-cycle perspective on V&V (i.e. validation activities precede and follow integrated system validation [ISV]); 2) division of the V&V process into several steps that focus on the different parts of the control room, as well as on the integrated control room; 3) a comprehensive approach (e.g. in addition to the HSI

and procedures it also includes artefacts such as requirements, style guides and training programmes in the scope of the V&V); 4) the use of a graded approach; and 5) the approach being requirements-based.

Table 2.1. **HFE V/V activities for the APR1400 MCR**

Stage	Activities	Objective
Stage 1 (1998) Development	Suitability verification (SV)	– Demonstrating no existence of a "show stopper" – Human engineering deficiency identification – Evaluate (advanced control room [ACR] man-machine interface [MMI] against conventional MMI)
	Preliminary validation (PV)	
Stage 2 (2000~2003) Development and design certification	PV1 (&SV1)	– Demonstrating basic adequacy for the various MMI resources – ACR issue testing – HED identification – Evaluate ACR MMI against conventional MMI
	PV2 (&SV2)	– Demonstrating that MCR ensemble fundamentally supports safety operation – ACR issue testing – HED identification – Evaluate ACR MMI against conventional MMI
	PV3	
	PV4	
	PV5	– Addressing the HFE issues raised by the regulatory body – HED identification
Stage 3 (2007~2010) Construction	PV6 (&SV3)	– Demonstrating that MCR ensemble supports safety operation and power production operation – Demonstrating basic adequacy for digital control system/programmable logic control MMI adopted – ACR issue testing – HED identification – Evaluate ACR MMI against conventional MMI
	PV7 (&SV4)	
	Final HFE V&V	– Final demonstration that MCR ensemble supports safety operation for the operating licence of APR1400 – HED identification

Source: Adapted from Shin et al., 2006.

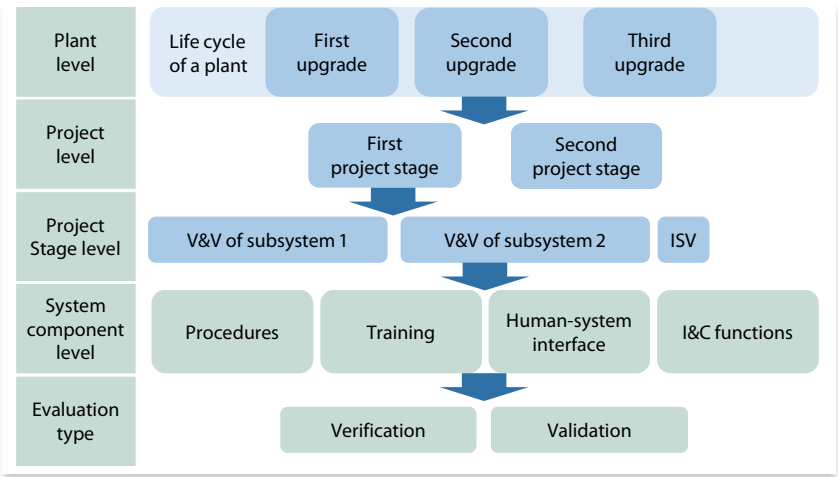
It should be noted that the Laarni et al. (2017) description of MSV suggests that the terms "stage" and "phase" can be used interchangeably. In describing their approach in greater detail, Laarni et al. (2017) note that the meaning of "phasing" depends upon the context/level:

- plant level – refers to different upgrades of automation and MCR systems during the life cycle of the plant;
- project level – refers to different project stages that are included in a single upgrade (categorised, e.g. in terms of whether the focus is on reactor or turbine side automation);
- project stage level – refers to test sessions that follow each other, in each of which a different set of MCR systems is assessed;

- system-component level – refers to individual elements and components of MCR work that can be evaluated in a single validation test session and that can be either verified or validated (evaluation-type level).

These phases/stages are depicted in the following figure.

Figure 2.1. **Hierarchical breakdown of V&V targets**



Source: Laarni et al., 2017.

2.2. Other relevant validation terms and methods

In Section 2.1, examples are provided of validations that were completed in multiple steps, highlighting the terminology that the authors used to describe their methods. Here, a few additional terms are identified that are considered to be important background information in the discussion on multi-stage validation.

Preliminary validation – The reader will have likely noted that Shin et al. (2006) used the term "preliminary validation" (PV) to describe validation activities that preceded their "Final HFE V&V". In describing their preliminary validations, they note that the PV1 test set included five integrated concept tests. The main purpose of the concept tests was to demonstrate that the basic approach to the individual HSI resources was sound. PV2 through PV4 were to contribute to demonstrating that the combined HSI system resources are fundamentally sufficient for safe operation. In addition, all PV tests provided the opportunity for the following:

- to confirm that design changes implemented since prior evaluations are effective and do not introduce new problems;
- to produce evidence addressing various high-level issues identified, which are related to the HSI system design;

- to identify remaining problems and opportunities to improve the HSI design;
- to compare human performance between APR1400 HSI and conventional HSI.

"Preliminary validation" is also a term that appears in Chapter 18, Attachment A of NUREG-0800, *Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants; LWR Edition* (NUREG-0800) (NRC, 2016). Attachment A, *Guidance for Evaluating Credited Manual Operator Actions*, provides guidance for an approach to crediting manual actions that is characterised in terms of four phases: analysis, preliminary validation, integrated system validation and maintaining the long-term integrity of credited manual actions. Although the guidance does not directly address the validation of an MCR design, like Shin et al. (2006), it presents preliminary validation as an activity that precedes ISV.

Sub-system validation – Laarni et al. (2017) use the term "subsystem validation" to refer to a validation activity occurring at the project stage level of their multi-stage approach to validation.

Integrated system validation – ISV is a concept described in multiple reference and guidance documents. NUREG-0711, Rev 3 provides a description and the following definition of ISV: "Integrated system validation is an evaluation using performance-based tests to determine whether an integrated system design (i.e. hardware, software and personnel elements) meets performance requirements and supports the plant's safe operation."

There are relationships between these terms and concepts. *Step-wise validation* as described by Bernston et al. (2004); *phased validation* as described by Hanada et al. (2010); and *staged validation* as described by Malcolm et al. (2000), Shin et al. and Laarni et al. (2017); are fundamentally the same concept. They all employ a series of validation activities beginning early in the design process and continuing up to, or (in the case of Laarni et al., 2017) beyond the decision to authorise operation. *Preliminary validation,* as used by Shin et al. and by the US Nuclear Regulatory Commission (NRC) in Appendix A to NUREG-0800, Chapter 18, is a more general concept to describe validation tests conducted prior to the last phase of testing to precede a decision to authorise operation. *Sub-system validation,* as used by Laarni et al. (2017) is a type of preliminary validation test applied to individual subsystems. The phase of testing preceding a decision to authorise operation is often identified as *Integrated System Validation*. Applications of an MSV such as those described previously in this chapter have employed ISV as one stage of a multi-stage approach.

2.3. Relationship between multi-stage validation and stepwise validations/modifications

Among the papers referenced in this chapter describing applications or models of multi-stage validation, Laarni et al. (2017) set forth the broadest conception, invoking a life-cycle perspective in which the stages or phases of validation begin early in the design conception and continue through initial plant operation, subsequent modifications, and presumably into decommissioning, although not explicitly stated. This view is consistent with the understanding that the validation

of a plant's ability to operate is a continuous process, but it nonetheless presents the following ambiguity regarding the notion of MSV: Phases/stages are defined differently at the plant, project, project stage and system-component level. As such, phase/stage, as used in a specific instance, may not be aligned with the use of the same term within other multi-stage frameworks. The principal challenge may be the application of the terms phase/stage at the plant level. Large modernisation efforts implemented over the course of three outages, for example, could be characterised as being validated through a multi-stage validation effort comprising three stages. These three "stages", however, would be quite different in meaning than the three stages described by Bernston et al. (2004), Malcolm et al. (2000), Hanada et al. (2010) and Shin et al. (2006). Further, one can assert that whereas there should be obvious links between the validation efforts for the three phases/stages of such modernisation, each phase or stage must be able to stand on its own merits as a basis for a decision regarding whether a plant can safely resume operation. Therefore, each phase or stage is a validation in its own right. To avoid confusion regarding the meaning of MSV and its potential applications, for the purposes of this report, modifications implemented in steps (i.e. including intervening periods of operation) are considered to have separate validations, rather than to collectively represent a multi-stage validation.

2.4. Relationship between multi-stage validation and design testing

In describing the merits of MSV, authors (e.g. Laarni et al., 2017) often note its natural relationship to and support of an iterative design process in which the results of early validation work are used to modify and enhance the design. Such descriptions raise the question of how MSV differs from design testing. While design tests and validation may invoke similar methodological practices and terminology, such as test design, scenarios and performance measures, there are important differences.

Design testing is used to provide information that is employed by the design team to make design decisions. Thus, the objectives of design testing can be quite diverse. Designers use testing to evaluate concept designs, test design options and trade-offs, and to refine detailed designs. For example, design tests can be used to determine if a new navigation strategy is usable by operators or to compare operator performance when using designs A and B to select the best approach. The results of design testing are fed back into the design process, and the problems and issues that are identified are addressed as the design work evolves.

Validations have more limited objectives. Validation tests assess whether an aspect of the design or the integrated design meets its intended purpose. To do so, validation tests use predefined criteria that identify the thresholds for acceptance that the objective has been met.

While design testing is conducted by the design team, validations are generally conducted by validation teams that have some degree of independence from the designers. While the two teams interact to conduct validations, the general design of the validation tests, for example how the design will be validated, and the conclusions to be drawn from them are made by the validation team without influence from the design team. Validations conducted in early design stages may

not require the same degree of independence as those conducted when the design is more mature (see discussion in Section 3.3 on MSV desirable characteristics).

Like design tests, when problems or issues are encountered, they can be addressed by the design team in the design process, and changes can be revalidated if necessary. Validation teams generally do not propose resolutions to design issues as that would compromise their independence. In general terms, the validation team identifies and describes the HEDs and the design team develops the design solutions to address the HEDs.

Design and validation tests usually differ with respect to the formality of how they are managed. Design tests can have informal requirements for test rigour and documentation. By contrast, validation tests typically have very formal requirements to ensure that they contribute to the achievement of overall validation conclusions and their acceptance as part of the regulatory process.

Design testing can therefore be viewed as having a formative purpose whereas validation has a summative purpose. The reader will find that the MSV as characterised in the remainder of this report should be conducted in a manner that allows the results to be used summatively (e.g. to enhance confidence in validation results and conclusions) but the approach can have formative benefits allowing interim results to contribute to a better overall design.

Chapter 3. What is multi-stage validation?

In this chapter, a proposed conception of multi-stage validation (MSV) in terms of high-level characteristics (i.e. defining characteristics and desirable characteristics) is set out. First, it is worthwhile to provide a brief statement regarding the fundamental concept of validation and the different ways that the term has been defined and understood.

3.1. Validation

Although there are many definitions of "validation", two of these definitions have been selected for illustrative purposes. Validation, as defined in NUREG-0711, Revision 3, is the set of activities to determine whether "a system can accomplish its intended use, goals and objectives in the particular operational environment." Validation as defined in International Organization for Standardization 11064-7 (ISO, 2006) is "confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application has been fulfilled."

Both the NUREG-0711 and the ISO 11064-7 definitions use very general terms to describe the process of validation (i.e. "set of activities" and "confirmation, through the provision of objective evidence", respectively). As such, both definitions are relatively non-restrictive with regard to the elements of the process that constitute validation. For the purposes of exploring the means to accomplish an MSV, an open view has been taken with regard to the activities that constitute validation, but only to the extent that they support the last clause of the validation definitions (i.e. confirming that, or evaluating whether, the system can accomplish its intended use, goals and objectives in the particular operational environment).

The final clauses of each of these definitions of validation are very similar in that they both identify the objective of validation as ensuring that, or evaluating whether, the system can accomplish its intended use and goals in the particular operational environment and that requirements for intended use have been fulfilled. This functional focus is an important characteristic of validation and a point of distinction from "verification". Verification, by contrast, is focused on ensuring that a design provides the support necessary to accomplish tasks while at the same time ensuring that it conforms to applicable human factors engineering (HFE) design guidance (Fuld, 1997). A simplified explanation of the difference between validation and verification is that validation focuses on performance of a design while verification focuses on characteristics of the design itself. Verification, as with other design and HFE activities, are presumed to be performed when and as needed and will only be discussed to the extent necessary to provide context.

An important distinction is whether "validation" is being used to describe a *process* with an intended outcome or the *outcome* of a specific process. For the purposes of this report, the term validation is used to refer to the *process*. The decision to use the term to describe activities rather than a conclusion for the purposes of this report was not arbitrary. The theme of the 2015 NEA workshop on control room validation was "Establishing Reasonable Confidence in the Human Factors Validation of Main Control Room Systems of Nuclear Power Plants". In the analysis of the results of the workshop (NEA, 2017), it is stated:

> The question of reasonable confidence is a complex one; and to address it, we must parse it into two considerations: what contributes to confidence in validation conclusions and at what point is that confidence sufficiently reasonable. In other words, are we addressing the right topics and have the topics been sufficiently investigated.

It is with this insight in mind that the distinction between validation as a process and validation as a conclusion is highlighted, with the present focus being on the *process* of validation, or more specifically on how MSV may contribute to confidence in the validation of the integrated system design. Had validation been focused on a conclusion, the matter of sufficiency of evidence and what is reasonable would be inextricable from such discussions, and these discussions would be further complicated by considerations of what is reasonable for which circumstances and stakeholders. It is not being proposed that such considerations be disregarded. On the contrary, the hope is that this report will ultimately shed light on what is reasonable.

The reader will find that validation activities as discussed in the conception of MSV could be performed at any point in the design development and operational life cycle, as long as performance implications of the design can be meaningfully addressed. As such, although the objective of a validation activity in the context of an MSV may be to support, through systematic accrual of evidence, validation conclusions concerning the overall system design, the subject of a specific validation activity may be an interim product of the design development/modification process (e.g. a conceptual design, a preliminary design and sub-sets of the full integrated design).

3.2. MSV defining characteristics

As described in Chapter 2, the notion of staged validation is not new, but it simply has not been formally defined such that the concept is universally understood. The purpose here is to set forth what is considered to be the defining and desirable characteristics of an MSV, not with the objective of limiting the concept, but rather of establishing a common ground for further technical dialogue on what an MSV can or should be and how it might be most effectively conducted. The fundamental concept is not elaborate and can be summarised by three defining characteristics:

1. MSV is conducted as a series of validation activities, each with its own objective(s), method(s) and result(s).
2. Each validation activity included within an MSV is designed to provide information that can be used as part of the basis for determining whether a

system can accomplish its intended use, goals and objectives in a specified environment.

3. Individual validation activities are conducted and grouped in time as stages that allow meaningful aggregation, summation or comparison of results, both within and across stages, to support interim or final validation conclusions.

The first defining characteristic captures the notion that MSV must comprise multiple unique validations. A single validation activity by itself could not be considered an MSV because it would not be a series. Similarly, multiple validation activities performed concurrently would not, by themselves, constitute an MSV as they would not be performed in a series. On this point, it should be noted that MSV does not preclude the performance of validation activities in parallel, but that such concurrent validation activities would only constitute validation at one stage of design. Finally, a validation activity that is repeated multiple times would not by itself constitute an MSV as the repetitions would share the same objectives, methods and results.

The second defining characteristic of MSV is that the activities it comprises are validation activities and only validation activities (i.e. the activities are designed to provide information that can be used as part of the basis for determining whether a system can accomplish its intended use, goals and objectives in a specified environment).

The third defining characteristic of MSV is that the validation activities can be associated or differentiated by commonality in timing. Common timing will most often be a common time of design development, where all tests are conducted within a period when the design has remained relatively unchanged. Tests conducted within this common period of design development would constitute a stage. A second but equally important criterion in this third characteristic is that the validation activities are conducted or grouped in a manner that allows meaningful quantitative aggregation, qualitative summation or comparison of the results, both within and across stages. This characteristic is fundamental to the notion of MSV as a process in which confidence is achieved by validation activities building upon the results of preceding validation activities and/or providing a foundation for activities in subsequent stages, and thereby increasing the depth of evidence provided. Conducting a series of validation tests at the same design stage may increase the scope of the validation but would not by itself be considered an MSV. However, if such tests were conducted in a manner to build upon the results of prior validation activities, the collective effort would meet this defining characteristic of MSV.

Although the preceding description of the third characteristic of MSV proposes that one stage of an MSV would likely be correlated with a stage of design, it should be noted that alternative conceptions of MSV stages are possible. For example, stages might be based on features such as subsystem functionality versus integrated system functionality (regardless of the design stage), accumulation of evidence, the realism and completeness of design and plant process representations, or by validation objectives. In the present report, MSV stages are discussed and exemplified as closely overlapping with design stages (for an example, see Chapter 4). This conception should be seen as an example of MSV stages for the purpose of this report. It is recognised that there will likely be practical and technical

rationales for justifying alternative bases and conceptions for defining the stages of an MSV. The concept of MSV is not limited to the specific stages discussed and illustrated herein.

3.3. MSV desirable characteristics

For validation activities to be considered an MSV as described in this report, the activities, collectively, must meet all three of the defining characteristics. Although the defining characteristics capture the task group's conception of MSV, it should be noted that meeting these defining characteristics should not be construed as defining a quality or acceptable MSV effort. Additional characteristics should be considered and satisfied to ensure a quality validation of a system design or design modification. The following are a few characteristics that are unique or particularly relevant to conducting an effective MSV. For more comprehensive and generally applicable guidance concerning the validation of systems at nuclear facilities, the reader should consult guidelines such as NUREG-0711 and standards such as International Electrotechnical Commission (IEC) 61771.

1. Validations are conducted from early (conceptual) to detailed (operational) stages of design development and operations.
2. The subjects of validation comprising an MSV include design concepts (e.g. operations, automation), system elements (e.g. subsystem designs) and the integrated design, and in general progress from system concepts and elements to the interactions and interrelationships of these elements as a sociotechnical system.
3. Results from each validation stage contribute to an accumulated body of evidence for validation of the final design.
4. Design changes made subsequent to a stage of validation are addressed through testing in the subsequent stage(s) of validation unless performance/safety is shown to be insensitive to the change or is bounded by the prior testing.
5. At each stage, validation methods, controls and rigour are commensurate with the intended use of the associated results and findings.
6. Validation testing of design elements that are novel, complex, or critical to safety is initiated early in the design process and confirmed in integrated testing.

Each of these six desirable characteristics is briefly discussed in the remainder of this subsection.

Validations are conducted from early to final (operational) stages of design development – Validation activities should begin as early in the design process as is meaningful and should be based on the chosen design process and early design decisions. This practice serves to ensure that deficiencies in the conceptual and early detailed designs are identified as soon as possible, enabling timely and effective resolutions and avoiding the cost and schedule challenges of introducing modifications late in the development process. Starting MSV activities early also allows designers to build

a larger body of evidence throughout the course of the MSV processes. Continuing validation efforts through deployment and operations (e.g. performance monitoring, periodic assessments) provides a means to ensure that the assumptions and conclusions of the validation activities conducted during the design process continue to be met during real world operations and the life of the plant.

It should be noted that the timing of initial MSV interactions and key decision points of the MSV process may be case dependent but should be appropriate so as to draw the types of conclusions necessary to develop a compelling argument of safe operation. For example, the balance between design and validation efforts early in the design process should be consistent with the demands of the design development effort (e.g. evolutionary versus revolutionary designs). This matter is discussed further under the discussion of desirable characteristics, below.

The subjects of validation generally progress from conceptual to detailed design and from the system elements to system interactions and interrelationships as a sociotechnical system – These two progressions can be considered separate and consecutive, since only under the detailed design stage can there be a progression from validation of system elements to validation of their interactions and interrelationships. That does not, however, mean that one should not keep an eye on concept-level issues at the later stages of design, but only that the focus will shift from whether the concepts themselves are valid to whether the successfully-validated concepts have been properly materialised.

One of the many challenges of validation is ensuring that all essential functions and important interactions are addressed in the validation process. MSV should be conducted in a systematic manner. Identifying and validating essential elements (e.g. subsystems) prior to progressing to more complex combinations of elements helps to: 1) ensure an adequate scope of the validation; 2) identify and differentiate performance effects directly stemming from system elements and those attributable to the context of or interactions with other system elements; and 3) increase the likelihood of successfully validating the integrated system.

Results from each validation stage contribute to an accumulated body of evidence for validation of the final design – An important means by which MSV can improve confidence in the validation of system designs and modification is by providing a framework for validation evidence to be identified and accumulated in a way that contributes to the validation of the final design. Early or interim validation results can contribute either directly or indirectly to the validation of the final design. Direct contribution might occur, for example, from the validation of a subsystem that is integrated, unchanged, into the overall system design. Validation results from the subsystem validation that are consistent with findings of performance associated with that subsystem during the integrated system validation (ISV) would enhance confidence that observations of performance associated with the subsystem during the ISV are valid. Conducting validations in a manner that supports this accumulation of evidence is a defining characteristic of an MSV. Obtaining the accumulated body of evidence is the desirable characteristic, and one not necessarily ensured by the defining characteristics.

Design changes made subsequent to a stage of validation are addressed through testing in the subsequent stage(s) of validation unless performance/safety is shown

to be insensitive to the change or is bounded by the prior testing. – A fundamental premise of MSV is that validation evidence can be accumulated throughout the design development process to support and further strengthen conclusions regarding the final validation of a design. This premise is challenged by the evolution of a design from its early concept to its final form. More specifically, design changes can render prior validation results irrelevant, or at a minimum, suspect with regard to their validity for the present design. Accordingly, an effective MSV effort must be conducted in a manner that optimises or at least facilitates the ability to determine the relevance of validations from preceding design stages to the current/final design. Conducting validation tests in a manner that provides results that are bounding (i.e. encompass) changes in performance that can be expected from subsequent design changes is one means to support the aggregation of results generated over time in the MSV process. The extent and effects of a design change may be difficult to predict or assess, and therefore a more tractable approach may be to retrospectively demonstrate through analysis or testing that the prior validation results are insensitive to the design change. Should neither of these preceding approaches prove to be desirable alternatives, subsequent validation efforts can be used to conduct a targeted assessment of the design change.

Testing controls are commensurate with the intended use of the associated results and findings – In order for MSV to support the competing goals of enhancing confidence in validation outcomes while ensuring the burden of validation is reasonable relative to its objectives, a graded approach to the MSV process is desirable. To be more specific, to apply the administrative rigorous controls associated with integrated system validation throughout the MSV process would enhance confidence in the validation outcomes but at a cost that would be difficult to justify. Rather, the task group believes that a reasonable approach to MSV, from both a technical and a resource burden perspective, would be tailoring testing controls (e.g. independence of the representative users/test administrator, fidelity of the testbed, detail/adherence to information collection procedures) throughout the MSV process. For example, ensuring tight controls early in the design process to limit variability resulting from factors outside the scope of interest may not be warranted when the design may undergo substantial changes or when a matter may be further addressed in subsequent validation efforts, potentially with stricter controls. By contrast, for instances where validation evidence will be limited or will not be subject to further validation, more stringent controls would likely be warranted.

For example, other test controls, such as those that ensure the independence of the validation team (from the designers of the system being validated) may be justifiably relaxed during early validation stages. Although a fully independent validation team could be used to validate early stage results, in some instances it may be sufficient to use less stringent measures such as a hybrid team (i.e. one comprised of both a design team and independent members) in conjunction with appropriate controls for the integration of team member findings for early validation testing. Designers should carefully consider the goal of the validation activity and determine the measures and controls necessary to achieve the goals of that particular test.

Validation testing of design elements that are novel, complex or critical to safety is initiated early in the design process and confirmed in integrated testing – In some cases, it

may make sense to focus on design work early in the process, minimising the validation work. This strategy may be justified for the development of evolutionary designs where the human interaction with the predecessor system is relatively well known. However, for designs that are novel, complex or critical to safety, it may be advantageous to start validation efforts earlier in the design process. This will allow a larger body of evidence to be developed throughout the design process that can be used during the MSV.

To summarise, the preceding lists of defining and desirable characteristics are not meant to represent a comprehensive list of characteristics that would typify an effective MSV. Rather, they are provided to stimulate thinking as to how these characteristics can be implemented and what other characteristics should be identified as necessary or desirable for contributing to an effective MSV.

3.4. Potential benefits of MSV

There are several reasons for using an MSV approach to validation, many of which are interrelated.

1. An MSV can help reduce project risks. MSV provides the design team with the opportunity to address issues (e.g. human engineering discrepancies [HEDs]) in a timely and cost-effective manner since they can be identified early in the design process. When problems are discovered late in the design process, as may be the case if only ISV is performed, they can be significantly more difficult to address and the solutions available may be more limited and suboptimal since key aspects of the design may be locked in. Discovering issues late in the process may also become "show stoppers" and threaten project schedules. The time necessary to design solutions that address the issues, implement them and revalidate them to ensure the issues are solved may delay other project activities such as operator training and licensing. By contrast, if issues are identified early, the design of solutions can proceed along with other design activities, and validation of the solutions can be integrated into subsequent validation evaluation.
2. When compared with ISV, MSV provides a more thorough validation since specific control room subsystems can be validated, such as those employing novel technologies or supporting risk-important actions, before they are included in the integrated human-system interface (HSI). Successful performance during ISV may mask deficiencies with individual subsystems, such as the alarm system, if operators can compensate for the deficiencies using other HSI subsystems. That is, subsystem HEDs may go undetected because operators overcome them when operating in the context of the full control room. ISV validates the integrated HSI design, and thus the effects of individual systems may not be clearly identified. Validating subsystems, especially those that are safety critical, complex or novel, helps minimise the possibility that such deficiencies are overlooked.
3. MSV can help overcome the methodological limitations of ISV, leading to a more robust validation. As discussed in point 2 above, ISV does not

specifically address subsystems. MSV makes longitudinal comparisons of subsystems possible as the design of the subsystem matures through successive modifications. Where such modifications are accompanied by performance improvement (e.g. fewer errors), it can be concluded that design changes have had the desired impact, or some of the potentials of the new design have become actualised. Additionally, ISV is limited in terms of the range of scenarios that can be examined. It is not possible to test all possible conditions of HSI usage during ISV. MSV provides an opportunity to increase the operational conditions that are examined during validation evaluations, providing a more robust evaluation.

4. Methodological improvements gained from incremental, sequential validation activities help to establish reasonable confidence in the validation of control room systems. A series of staged validations provides validation teams with experience developing validation scenarios, using performance measures and defining acceptance criteria so that ISV can be conducted more efficiently and with greater validity. That is, conducting validation tests prior to ISV provides an opportunity for the validation team to check and improve the test methodology, thus reducing the risk of encountering difficulties during ISV and improving confidence in the validation results. For example, performance measures can be tried and replaced if they are difficult to use, are insensitive or otherwise do not work out.

Taken together, the advantages of MSV, relative to validation of the final design alone, should provide a basis for increased confidence that the design is suitable for its intended purpose. However, gaining the full benefit of MSV, particularly with regard to enhancing confidence in the final design, will depend on appropriate co-ordination of validation activities, integration of the results, and documentation of the MSV process and results. As such, MSV plans should include sufficient time and resources to allow for the proper conduct of the validation activities and resolution of interim validation findings through the design development process.

Chapter 4. Illustration of a staged approach to validation

In Chapter 3, an overview of how multi-stage validation (MSV) has been defined for the purposes of this report (i.e. the defining characteristics) is provided, along with some of the possible characteristics that would contribute to an effective MSV (i.e. the desirable characteristics). In this chapter, the aim is to make these concepts more tangible by way of an illustrative example of how an MSV might be structured and a description of the activities it would entail.

4.1. MSV and its relationship to system design and life-cycle stages

As previously discussed, the third defining characteristic of MSV is that individual validations are conducted and grouped in stages that allow meaningful aggregation, summation or comparison of data, both within and across stages, to support interim or final validation conclusions. It is proposed in the discussion of this characteristic that stages might be defined by commonality in timing and that a basis for common timing is that the validations within a given stage all occur during a period where the design remained relatively unchanged. With this perspective in mind, the stages of an MSV are not so much stages of validation as they are stages of design during which time validations might be conducted. As a result, all validations within a stage have roughly the same design, or level of design development, as their shared reference point. This approach has the advantage of allowing MSV to be flexibly applied to each design team's specific approach to design development, or to design process variations that are necessary to accommodate the demands or constraints of a specific design project, rather than attempting to establish a stage construct that might not map well onto all such possible variants. It is also expected to support aggregation, summation and comparison of validation results within a design stage.

4.2. Example stages and activities of MSV

To construct an example MSV in which validation activities are grouped on the basis of design development stages, the NEA task group began with design stages as described in International Organization for Standardization (ISO)/ International Electrotechnical Commission (IEC) 26702 (IEEE Std 1220-2005), "Standard for Systems Engineering – Application and Management of the Systems Engineering Process". The standard describes the application of systems engineering throughout the system life cycle, and specifically with respect to following the design stages: *System Definition; Preliminary Design; Detailed Design; Fabrications, Assembly, Integration and Test;*

and *Production and Support*. To illustrate the MSV concept, the same design stage construct was generally followed, but the characterisation of stages was maintained at a fairly high level for the purposes of the illustration. When applied to a specific design programme, the actual stages should reflect those that are applicable to the design and not generic stages.

Table 4.1 summarises the example of how a multi-stage approach to validation can be applied during the life cycle of a design. Column 1 of the table identifies the stages of design within which validation activities can be performed. Each of these stages is addressed as a row in the table. Note that there are additional stages in the design process, such as human factors engineering (HFE) analyses and requirements development; however, the example has been limited to describing potential validation activities beginning with the design concept through deployment and operations.

Table 4.1. **Example multi-stage validation stages and activities**

Design stage	HFE activities	Validation objectives	Example claims	Relationship to other activities
Concept design	The HFE activities typically performed at this stage include, but are not limited to, supporting the development of a design concept that meets the overall concept of operations and functional requirements.	Provide sufficient evidence that the design concept meets the overall concept of operations and functional requirements.	The HSI concept and the procedure concept provide co-ordinated (integrated) principles for supporting the requirements for crew's situation awareness and performance of control actions. Concept for control room layout is co-ordinated with concept for instrumentation and control safety classification and supports crew situation awareness as required by the plant safety and operational concept.	A validated concept design basis supports detailed design and integration. The validation of the concept design may provide feedback to the earlier HFE activities.
Sub-system design	The HFE activities typically performed at this stage include, but are not limited to, supporting preliminary design of subsystems such as alarm, display, control and procedure subsystems.	Provide sufficient evidence that the subsystem designs achieve their intended purpose.	Subsystem designs achieve their intended purpose and are ready for integration into a complete design. The alarm system supports the crew/operator in attending to the important functions/systems/components and down-prioritising those of minor significance, in all plant conditions. The overview information supports the crew in monitoring and interpreting the overall plant process development and supports the teamwork requirements (of the conduct of operation).	Validated subsystems are ready for integration into a complete control room design. The validation of the subsystem designs may provide feedback to the earlier HFE activities.

Table 4.1. **Example multi-stage validation stages and activities** *(cont'd)*

Design stage	HFE activities	Validation objectives	Example claims	Relationship to other activities
Integrated system design	The HFE activities typically performed at this stage include, but are not limited to, supporting the integration of subsystems into a complete final design.	Provide sufficient evidence that the integrated system design (i.e. hardware, software and personnel elements) meets performance requirements and supports the plant's safe operation.	The integrated design supports the crew in preventing situations that can lead to transients and initiating events, e.g., the crew can detect, understand and evaluate potential problems in due time to be able to perform preventive actions. The integrated design supports the crew in mitigating transients and initiating events by enabling the crew to sufficiently supervise and understand the status of safety systems and safety functions. Operator workload is within acceptable bounds for all event classes. The integrated design supports operators in ordinary operation tasks (e.g. start up, shut down), surveillance and monitoring of status, identification and diagnostics of deviations, maintenance and testing of systems and components. The HSIs minimise personnel error and support error detection and recovery when errors occur.	The validated integrated design can be deployed into operational settings and provides the performance basis for monitoring programmes. The validation of the integrated design may provide feedback to the earlier HFE activities.
Deployment/ operations	The HFE activities typically performed at this stage include support programmes to identify design deficiencies and opportunities for design changes to maintain and improve operational performance and safety.	Provide ongoing evidence that the design (as built, maintained and operated) continues to support the plant's safe operation and identify opportunities for design improvement.	Design deficiencies and improvements have been identified.	Validations within performance monitoring programmes provide a basis to have confidence that performance will be maintained and that the need for design modifications will be determined.

The second column identifies the types of HFE activities that may take place for each design stage. Individual design programmes may include some or all of these activities and may be subject to validation. The third column identifies the general objectives of validations performed at each stage. The objectives are different depending on the design stage, but all of the objectives generally relate to showing that the HFE activity or design achieves its intended purpose. Sections 4.3 through 4.6 below provide examples of the types of validations that can be performed at the different design stages. It is not the intent to suggest that a multi-stage approach should necessarily contain all of the individual validations. The specific validations included in a design programme should be identified by the design team and tailored to the needs of the programme.

The fourth column identifies the types of claims that can be made by the validation team once validation is completed. Claims are assertions that the validation objectives have been achieved, or more simply stated, claims are conclusions that are drawn from the facts (i.e. the evidence). The soundness of the connection between a claim and the supporting facts (i.e. the justification or reasoning behind why the evidence supports the claim) plays a critical role in the establishment of reasonable confidence.

The fifth and final column identifies the relationship of validation activities at each stage with validation activities at other stages and the overall validation of the design. It is important to underline that MSV is a process in which individual validations at each stage contribute to the ultimate validation of the design. Thus, validations build on each other to create reasonable confidence that the design achieves its intended purpose. One can be reasonably confident that a control room design based on a validated task analysis, for example, will reflect actual task requirements.

4.3. Concept design

The HFE activities typically performed at this stage include, but are not limited to, supporting the development of a design concept that meets the overall concept of operations and functional requirements. Although the HSI concept design is an important area of focus for HFE, other design concepts should be addressed, including:

- operating concept design;
- automation concept design;
- crew concept design;
- procedure concept design.

Based on the requirements, the feasibility of each concept design will be estimated and then developed up to testing and the first validation level. In this manner, the MSV approach can include the first validations of a concept design.

At the design concept stage, one objective can be to establish a connection between the task analyses and the future subsystems as described below, in particular if these concept designs are innovative or have significantly evolved from the existing system.

From a methodological point of view, MSV involves many different aspects. A few of these are highlighted below.

- A comprehensive approach is recommended, which implies that for each concept design, one should define a satisfactory mock-up for the concept design validation. MSV at the concept design stage can be performed in static mock-ups (layout, paper procedure), dynamic mock-ups, or more sophisticated simulators, more or less representative of the future process according to progress in the design.

- The simulation conditions of the MSV would likely need to combine several elements (subsystem, procedure, layout, etc.) of the design. For the development and validations of design modifications and evolutionary designs, these would likely include a combination of existing/predecessor design elements and some of the future design. The validation testing can be done per concept design or could associate two or more concept designs. The latter case would support greater confidence in the results since the interaction between different concept designs and their consequences in the probable future operating activity will be observed simultaneously.
- As noted above, it is recommended to establish connections between the task analyses and the new concept design, in particular for the tasks identified as critical. The critical tasks, or at least a subset, should guide the validation of a concept design in order to validate the new concept design as a feasible, functional integration of the design requirements. The more complete the concept design is with respect to incorporation of design requirements, the more value the concept design validation can provide for validating the requirements as comprehensive and sufficiently detailed.
- Both task analysis and operating experience can guide the MSV process, including the validation of concept designs. Whether for design modifications or new build, these analyses support the identification of critical tasks and the range of normal, abnormal and emergency operation situations in which a concept design has to be tested and validated.
- Specific criteria should be defined for the MSV concept design. For instance, for an HSI concept design, relevant criteria would be their usability and utility; for a crew concept, design-relevant criteria would be the human resources, task allocation and workload. For an automation design, the feedback for the end user and the manual controls will be fundamental for their validation.
- Validation of a concept design can be based on "before-after" comparisons, or comparisons of two concept designs in order to demonstrate their advantages and disadvantages, and to address the results as benefits in terms of human performance and safety. The results in terms of advantages-disadvantages can be articulated to a risk analysis based on the results of the simulations conducted in the MSV frame, but also based on the literature, the operating experience or the probabilistic safety assessment, for instance.
- Results from this stage may also be useful in identifying knowledge and skill requirements associated with any new technologies introduced as part of the concept design.

The concept design options have to be discussed and different points of view considered, including: the end-user adequacy, the safety requirements, the design constraints and the operations standpoint. From this perspective, even if validation testing and design testing are viewed as two separate activities, at this stage it is important to establish a relationship between them. Validation of a concept design is more predictive and uncertain than demonstrative and definitive. More specifically, a comprehensive validation can be difficult or even impossible, even if

the concept validation is based on a set of scenarios representative of the uses and operating conditions anticipated for the system under development. The results can be partial or concept by concept. As a consequence, particularly for new build projects, the validation of a concept design will likely require confirmation or completion in subsequent MSV stages.

4.4. Subsystem design

The HFE activities typically performed at this stage address various subsystems, provide evidence that those subsystems achieve their intended purpose and are ready for integration into a complete design. Subsystems that would become targets of validation are based on any well-founded division of a control room system or other plant HSIs into lower-level entities. As a result, the targets of subsystem validation may vary depending on the specific project or state of the project. The aim is both to provide support for iterative control room design and to conduct a thorough safety validation at the subsystem level.

The following issues are addressed in this section:

- interplay between subsystem design and the preceding and following design stages;
- organisation of test activities;
- inventory of evaluation targets;
- test condition selection;
- development of evaluation criteria;
- testbeds;
- review process.

Connections must be established to the preceding and following design stages. Connections are built to the concept design phase, and the results of the concept design phase must be carefully reviewed in preparation for subsystem validation activities. In particular, an evaluation should be made to ensure that the concept of operations has been applied to all subsystems consistently. Similarly, outputs of validation at the subsystem level should provide input to the planning of validation at the integrated system stage. Tests targeting the validation of clusters of interrelated subsystems could serve as a pilot test for testing at the integrated system validation (ISV) stage. They could also provide guidance for focusing ISV test efforts on those systems that need more detailed evaluation and support the interpretation of ISV test results.

Test activities should be carefully scheduled, and a systematically organised hierarchy of test activities should be established. It is important for plant simulation models, alarms, HSIs and emergency operating procedures to have been developed to a sufficient extent. For example, procedure verification should be conducted before a specific procedure is used in subsystem validation.

At this stage, there are typically multiple test sessions. First, there could be a continuum from testing individual subsystems (e.g. alarm, display, control and procedure subsystem) to testing clusters of subsystems (including a set of alarms, displays and controls needed in the execution of a particular emergency operating procedure). Second, validation efforts at a particular phase of subsystem design can be divided into several test events, during each of which a small subset of systems is tested.

Human factors engineering activities at this stage should be based on the hierarchical organisation of systems: for example, HSIs can be divided into several hierarchical levels, ranging from individual display formats and pages to workstations. Since it is not possible to validate all subsystems thoroughly, the main effort is placed in the evaluation of the most critical systems (i.e. a graded approach is applied). The HFE work is typically tailored according to some critical dimensions, such as safety criticality, complexity and novelty of the subsystems. All of the new safety HSIs and emergency operating procedures should at the very least be comprehensively tested in several successive test events. One option is to test safety-critical systems one cluster at a time.

Human factors validation at the subsystem stage can be based on four kinds of reference. In most cases, validation is a requirement or is normative referenced, but could also be an expert-judgement, or even benchmark referenced. In addition, subsystem validation could also be called concept-referenced, i.e. the new design is evaluated against the explications of the concepts described in Section 4.5, and the acceptance of the design is based on a set of criteria that are derived from these explications.

Different kinds of testbeds and facilities, varying in physical and functional fidelity and dynamics, can be used in subsystem validation. Typically, subsystem validation is performed either in a dynamic simulator environment (e.g. engineering or training simulator, virtual or augmented reality environment) or with a static mock-up. Fidelity of the testbed should increase as the maturity of the design increases.

4.5. Integrated system

Conducting an ISV at the end of a design development process is assumed in the prevailing HFE frameworks and guidelines. In the context of an MSV, the ISV is still relevant and necessary. MSV does not eliminate the need for testing the integrated system as is the focus in ISV, but rather subsumes ISV in a way that can improve the efficiency and effectiveness of ISV. The purpose of ISV is to show that the *integrated* system meets performance requirements and supports the plant's safe operation.

When validation is conducted as a series of activities, including ISV, ISV can also serve the purpose of assessing whether issues that have been detected in earlier stages have been effectively dispositioned. For example, it can address whether the actions taken to address problems identified in earlier stages (e.g. subsystem validation) have been effective. In this sense, an ISV within an MSV process does not start from scratch. Instead, it is a means to determine whether issues that have been

tracked have been resolved. Additionally, validation results from earlier stages might provide the basis for reducing the focus in ISV on performance with systems that have been stable and well validated in earlier stages. In such instances, using validation results from earlier stages could allow the ISV to focus more on: 1) matters associated with the integration of validated systems rather than fundamental usability (e.g. aspects of system use that are dependent on co-ordinated use with other systems) and 2) systems that have received less attention in earlier validation activities.

Within the context of MSV, ISV could:

- test the ability of the integrated system to meet requirements not sufficiently tested as a result of limited integration, limited simulation capabilities and limited operator competence at previous stages, for example;
  - workload, staffing and team organisation in full-scale demanding situations;
  - global situation awareness;
  - usability and performance support of the integrated HSI;
  - performance during complex, full-scale scenarios;
- test the ability of the integrated system to meet requirements added or to be substantially modified based on experiences from previous stages;
- assess issues identified in previous stages based on safety relevance and confidence in results from previous stages, for example confidence in how representative the previous validation results are for integrated functioning of the control room.

4.6. Deployment/operations

During the "deployment/operations" stage, performance as validated in earlier stages, is monitored and maintained. As such, performance monitoring and assessment activities during deployment and operations can provide validation of the design as tested and can be of value in monitoring the incremental impact of changes in design or operation that occur throughout the life cycle of the facility. Such activities can be particularly beneficial for validating performance under conditions that may be difficult to assess or approximate in a simulated setting (e.g. sustained operations, extensive operating experience with the system). As noted in Table 4.1, the HFE activities typically performed at this stage include, but are not limited to, supporting programmes to identify design deficiencies and opportunities for design changes to maintain and improve operational performance and safety. Operating nuclear plants have programmes, both continuous and periodic, to address potential challenges to performance and to foster improvements. For these programmes to achieve their intended purpose, they should:

- be sufficiently thorough and rigorous to identify issues and potential improvements and capture important production and safety challenges;

- identify issues associated with all important impacts on performance, for example HSIs, procedures, training, operational practices (such as shift turnovers), and organisational factors;
- use multiple sources of information, such as operator interviews and performance trend analyses;
- document results with sufficient detail and in a format that will support activities to address them;
- enable the plant staff performing the analyses (e.g. conduct root cause analyses and identify corrective actions) to produce reliable, reproducible results.

As part of MSV, such performance monitoring and assessment activities during deployment and operations can confirm or disconfirm assumptions and conclusions of the design and validation process and provide a basis for when/whether design modifications may be warranted.

Chapter 5. Integrating results and drawing conclusions

The goal of human factors engineering (HFE) validation is to provide reasonable confidence that a design is suitable for its intended purpose, meaning that the design supports production and safety missions. Multi-stage validation (MSV) is an approach to meeting this goal through incremental, successive validation activities beginning early in the design process and continuing to design completion and use. When using an MSV approach, a significant challenge becomes how to define and structure the validation activities so that the results can be adequately integrated together in order to achieve an overall conclusion about the design's validation.

Koskinen et al. (2017) developed an approach to integrating the results of multiple validation tests called the "Systems Usability Case" (SUC). This approach is based on their "Systems Usability Framework" (SUF; Savioja and Norros, 2013). SUF is a human performance model developed to evaluate the systemic effects of new human-system interfaces (HSIs) and other tools within complex sociotechnical systems. SUC extends SUF by comprehensively considering all validation tests for a specific design within the broader perspective of safety case methodology (e.g. ONR, 2013). An appealing aspect of Koskinen's SUC is that, while their application of SUC uses the SUF, the basic framework is not dependent on it and can be used with other models of human performance in complex systems that designers may rely on.

The SUC approach consists of two main parts, a goal structure and a claim structure. The goal structure is generated prior to the specification of validation test activities. Reflecting safety case approaches, the goal structure identifies the information needed to make the safety case for the design's acceptability. The goal structure also provides a framework for linking (integrating) individual test activities to the high-level goal of design validation. In Koskinen et al.'s framework, high-level goals are decomposed into both systems usability and plant-specific sub-goals[3] and associated acceptance criteria that demonstrate that the sub-goals are achieved. One example of a sub-goal is, "If the main control room cannot be used the unit shall be able to be operated to safe state by using safe shutdown procedure." Its associated acceptance criterion is "the unit can be operated to safe state (outlet temperature of core less than 140°C)."

3. Koskinen et al. (2017) note that high-level goals are "divided into several sub-level goals, i.e. into SU (systems usability) and plant-specific requirements." We prefer the term "sub-goals" rather than requirements, so they are not confused with detailed design requirements that are developed during the design process.

Collectively, these sub-goals describe the information required to validate the design. While the goal structure is generated before testing begins, it can be modified during design development as new sub-goals are added or removed based on the results of validation tests or changes to the detailed design as it evolves.

Validation tests are designed to provide the information needed to determine whether the sub-goal is achieved, i.e. the acceptance criteria are met. For the example sub-goal above, a test condition can be developed for a scenario involving loss of main control room because of fire. Validating one sub-goal may require more than one test.

The SUC framework developed by Koskinen et al. (2017) lends itself to an MSV approach to validation. This is because: 1) the framework is predicated upon the use of multiple validation tests; 2) the sub-goal structure may include tests that do not focus on the full, integrated system design; and 3) the framework is not tied to a specific approach to design stages and thus can conform to the stages employed in a particular design project. An example of the type of validation that may occur prior to integrated system validation (ISV) is that of a novel alarm system that includes new alarm processing approaches and alarm information displays. Validating such a novel system may be performed at the subsystem design stage and may be one sub-goal necessary for making the overall safety case. Validating one aspect of the HSI is difficult within the context of the fully integrated system because, as discussed earlier, operators may compensate for design deficiencies of one part of the HSI by using other HSI resources. To validate the alarm system, it should be tested prior to system integration.

Koskinen et al. (2017) describe the claim structure as the mirror image of the goal structure. The principal elements of the claim structure are evidence, arguments and claims, with the claims corresponding to the sub-goals within the goal structure.

Validation results are characterised as evidence. An item of evidence is a description of operator performance in the context of a particular operational condition. Items of evidence may be either positive or negative from the point of view of the design depending on whether the corresponding acceptance criterion is met or not. Positive evidence exists when acceptance criteria are met. These are referred to as “human engineering consistencies” (HECs). When the acceptance criteria are not met, the human engineering discrepancies (HEDs) are identified. The HEDs are evaluated and resolved, where appropriate, and the resolutions may be validated in subsequent tests.

The assumptions and implied judgements that are inherent in the evidence need to be clearly presented and defended. Arguments, therefore, are key to the claim structure as they provide the reasoning for how the evidence supports or rejects a claim. They are thus the validation team’s interpretation of the results for each test with respect to the sub-goals. The final task is to connect the arguments for each validation test to their sub-goals, to other related sub-goals and to the higher-level goals regardless of the stages in which tests are conducted to form a conclusion as to the design’s overall validation and acceptability. Conclusions regarding any one sub-goal may be based on multiple tests. When some of those tests lead to the HEDs, the tests become part of the design’s rationale. The results from individual tests are not eliminated or ignored.

Considering the SUC framework as a whole, it provides a structured approach to operationalise the intended purpose of the system to be validated, define acceptance criteria, connect this to validation data and document it all in a way that allows transparency (e.g. for a governmental regulator) of the rationale and basis for the validation conclusions.

Chapter 6. Documenting a multi-stage validation

To support confidence in the results of a system validation, designers can build a portfolio that establishes the basis for the validation conclusions through a collection of documents that describe and logically integrate the rationale, conduct and results of validation activities. These validation activities could include validations based on testing, operating experience or analysis. For example, the International Atomic Energy Agency (IAEA) identifies such a range of sources of evidence to support the dependability assessment of software for safety instrumentation and control (IAEA, 2018). Similarly, the multi-stage validation (MSV) portfolio might also include other information, such as risk analyses, operating experience that can help substantiate the appropriateness of the MSV approach taken and results obtained. With respect to the documentation of an MSV approach, the portfolio could include validation results from conceptual through integrated design. For example, including the validation of the analyses of risk-important actions can provide assurance that such actions have been identified, increasing confidence that important actions have not been overlooked and that they have been appropriately evaluated. Inclusion of early validation activities in the validation portfolio can also provide assurance that the performance observations during the integrated system validation (ISV) are representative (i.e. when performance observations in the ISV affirm findings from earlier validation activities) and that collectively the validation results address all important functional requirements.

To fully derive the benefit of MSV with respect to increasing assurance of validation outcomes (i.e. confidence not only within the design team but also among other stakeholders, such as customers and regulators), the MSV portfolio should reflect the breadth of validation activities conducted. It should also include the basis for why these activities represent an assessment that is sufficient in depth and scope for judging the suitability of the design for its intended purpose. To this end, it is proposed that the portfolio include information to address the following:

- Scope of the system validated and the validation objectives
  - The system that was validated should be defined with regard to its key elements (e.g. hardware, software, personnel and environment) and its boundaries such that the scope of the system validated can be commonly understood.[4]

4. Note that the importance of defining the scope of the system to be validated increases when the scope of validation testing does not encompass the entire system as might occur in a graded-approach or when elements/subsystems are excluded from testing as a result of a proven history or low importance.

  - The objectives of the validation should be stated in sufficiently specific terms so that they can be commonly understood and reliably assessed against validation results. The objectives should be presented in a form that shows their relationship to the validation of the system (e.g. the hierarchical relationship of lower-level specific objectives to broader, higher-level objectives).

- Scope of testing conducted and basis
  - The scope of system elements and operational conditions/actions/tasks to be tested should be identified and the rationale for why the scope of testing is sufficient to support validation of system should be provided.
  - Any elements/subsystems of the system that were not specifically addressed through the validation testing should be identified, the method (e.g. validation based upon analysis or operating experience) identified and the basis for using an alternative to validation testing provided.
  - If a graded approach was applied to the validation, the approach and its basis should be described.

- Testing methods and controls employed and their bases
  - The test methods (e.g. testbeds, participants and procedures) that were used and the controls/rigour applied to their implementation should be identified. The basis for their adequacy should be addressed (e.g. if lesser controls were applied to earlier stages than later stages, the basis for this approach and the implications for interpretation of results should be described).
  - The measures and acceptance criteria that were used should be specified and a basis for their acceptability provided (e.g. appropriateness of margins given reliability requirements/safety considerations).

- Analysis methods and bases
  - The methods used to analyse the MSV results should be documented in sufficient detail to support examination.
  - Where the analysis is based upon results from multiple validation activities, the basis for aggregation, summation and comparison of data across these activities should be provided.
  - The analysis documents to what extent project-specific validation methodology has been systematically adapted to effectively address the actual requirements and design solutions. For example, the requirements and test criteria have been clarified, test scenarios and observation protocols have been adapted and completed according to the results and insights gained during the MSV process.

- Conclusions and their bases
  - The validation conclusions drawn, whether from testing, analysis or operating experience, should be clearly stated, as well as how the analysis of results supports the conclusions in sufficient detail to support examination.
  - The conclusions drawn from validations are supported by the depth, consistency/convergence and stability of results such that they can be judged predictive of future performance.

The uncertainties associated with any validation conclusions should be explicitly stated and the implications that such uncertainties have for the continued development and validation of the design should be identified. This information is important at each validation stage in order to effectively resolve any uncertainties and associated risks.

Chapter 7. Conclusions

Multi-stage validation (MSV) is a systematic approach to validating complex systems and modifications to such systems. It is considered a longitudinal approach that achieves validation through a series of co-ordinated validation activities that incrementally build a case for the validation of the final design solution. A mature and well-guided MSV approach has the potential to provide value in several ways:

- MSV provides the design team with the opportunity to address issues (e.g. human engineering discrepancies [HEDs]) in a timely and cost-effective manner since discrepancies can be identified early in the design process. An MSV approach thus reduces risk in the design process.
- By including early validation stages prior to the integrated system validation (ISV), MSV provides a more thorough and robust validation than ISV alone since individual control room subsystems can be validated under controlled and focused test conditions.
- By conducting validations at multiple stages, MSV provides the opportunity to use a larger number of scenarios over the course of the design development, thereby conducting man-in-the-loop tests for a broader range of tasks and operational conditions.
- MSV enables longitudinal comparisons of subsystems as the design of the subsystems matures through successive modifications.
- A series of staged validations provides validation teams with experience developing validation scenarios, using performance measures, and defining acceptance criteria and other aspects of methodology so that the validation of integrated final design can be conducted more effectively and efficiently.

Although a phased or staged approach to validation is not an entirely new concept, guidance for and experience with its application are relatively limited. Through the development of this report, the task group of the NEA Working Group on Human and Organisational Factors (WGHOF) sought to discuss issues and identify approaches that may aid future guidance development and implementation activities. The process of developing this report included many vigorous and thoughtful discussions among task group members, as well as careful consideration of the invaluable input of the experts who reviewed the preliminary draft of this report and challenged or broadened the group's views during their participation in the 2017 workshop that conducted during the second phase of the development of this report. Through these interactions, it came to be recognised that although MSV has promise, effective and efficient implementation of an MSV is likely to present certain challenges, namely:

Optimising the boundary between design and validation – Section 2.4 provides a brief discussion of the relationship between an MSV and design testing. The motivation for including this kind of discussion was drawn from task group debates about the similarities, differences and relationships between these activities and how MSV could be most effectively implemented. The question evoked was how to both support the design process and achieve reasonable confidence in the MSV without unduly burdening the creative design process with the administrative controls and overhead of formal validation activities. Many of the invited experts shared this concern at the workshop, and although the present report was revised to temper the discussion on early validation activities, it is expected that until additional experience is gained, design and validation teams will have to meet the challenge of establishing the methods and processes that strike an optimal balance.

Maintaining the boundary between design and validation – Closely associated with, and perhaps a subset of, the challenge described above is the matter of independence between design teams and validation teams. The majority of text books and guidance documents, including the US Nuclear Regulatory Commission's NUREG-0711, recommend independence between the design and validation teams to ensure objectivity in the conduct of validation activities and assessment of the results. Implementing an MSV will likely challenge most organisations' capability to strictly adhere to such guidance as the burden of maintaining a fully independent team of qualified individuals to conduct multiple stages of validation, potentially ranging from conceptual design through the ISV, would be substantial. Graded approaches to independence or alternative methods for controlling potential bias in the validation will be practical necessities. This matter was briefly touched upon in Section 3.3, MSV Desirable Characteristics. It is noted in this chapter that one characteristic of an effective MSV is that validation methods, controls and rigor are commensurate with the intended use of the associated results and findings at each stage of validation. Potential solutions, such as validation teams that include individuals who are not independent of the design team, will likely challenge the boundary between design and validation and the basis for confidence in the validation conclusions.

The dynamics of the MSV process and integration of results – Section 3.2 proposed three defining characteristics of MSV. The third defining characteristics was that:

> Individual validation activities are conducted and grouped in time, as stages, that allow meaningful aggregation, summation or comparison of results, both within and across stages, to support interim or final validation conclusions.

On the surface, it would seem possible to be successful in designing and implementing a validation that meets this defining characteristic by applying systematic and logical methods for system decomposition, evaluation and analysis. In practice, however, it is more complex in that a system in development, as is the case during an MSV, is a system that is evolving. As a consequence, the target of MSV is likely a moving target. Changes in the design over time will influence the specific validation plans and challenge the ability to readily integrate results of early validation activities with those conducted when the design is more mature. For this reason, Section 3.3 listed the following point among the characteristics of an MSV that should be sought to establish an acceptable MSV:

> Design changes made subsequent to a stage of validation are addressed through testing in the subsequent stage(s) of validation unless performance/safety is shown to be insensitive to the change or is bounded by the prior testing.

It is expected that validation teams may face logistical, schedule and budgetary challenges in keeping with this characteristic.

In addition to the challenge of addressing *what results can be aggregated,* there is the matter of *how the results should be aggregated*. The latter question is more a conceptual than an interrogatory matter concerning the definition of the goals and sub-goals of the validation and the evidence that should be brought to bear with respect to those goals. Chapter 5 describes the Systems Usability Case developed by Koskinen et al. (2017) as a possible approach to addressing this matter of structuring the analyses and integrating the results. Given that the approach has only recently been developed, it is expected that there will be a learning curve associated with its application.

Acceptance of the final design – In 2017, the NEA published the proceedings of the Experts' Workshop on Human Factors Validation of Nuclear Power Plant Control Room Designs and Modifications (NEA, 2017: 49). In the report, it was noted that:

> The question of reasonable confidence is a complex one; and to address it, we must parse it into two considerations: what contributes to confidence in validation conclusions and at what point is that confidence sufficiently reasonable. In other words, are we addressing the right topics and have the topics been sufficiently investigated.

Achieving reasonable confidence is not a challenge that is unique to the MSV, but rather one that may be addressed well by MSV. It is believed that applying an MSV approach that: 1) has the defining and desirable characteristics described in the present report; 2) employs a systematic approach to structuring analyses and aggregating results, such as the systems usability case approach; and 3) is presented in the context of a portfolio of supporting documentation as described in Chapter 6, should provide confidence in the validation results and lay the logical foundation for a case that the validation is sufficiently reasonable, or more simply, sufficient. Although the determination of what is "sufficient" will be dependent on many factors, such as the characteristics of and experience with the system or modification to be validated, a validation approach that is conducted and presented as described above should provide a clear basis for stakeholders to engage in a meaningful dialogue concerning whether a validation is sufficient.

Chapter 8. **Recommendations**

Looking ahead, there is potential for multi-stage validation (MSV) to become a mature approach to the validation of control room designs. At present, the nuclear industry is witnessing an increased interest in small advanced reactor designs, (e.g. liquid metal and high temperature gas reactors). The substantially different size, technology and operation concepts for and uses of these reactors, relative to large light water reactors, will reveal gaps in the available knowledge and experience that can be brought to bear in the development and licensing of these technologies. These gaps will likely be drivers towards the use of staged validation as a means to gain confidence, both in terms of the developers and the regulators, that these new technologies can be efficiently brought to market and safely operated.

The preceding chapter noted several challenges that remain when planning and implementing MSVs. It is expected that these challenges can be addressed and resolved through the experience and insights that will be gained by conducting MSVs for a range of validation applications. Design and validation teams implementing staged approaches to validation will, as a matter of necessity, develop means to address the planning and implementation challenges involved in MSV. Broadly sharing the methods employed and lessons learnt from conducting MSVs, particularly with regard to addressing these challenges, will be important for continued development and widespread adoption and implementation of MSV in the nuclear power industry. Future initiatives should support technical exchanges on MSV methods and experience and the distillation of lessons learnt into practical implementation guidance.

Two potential areas of emphasis for future technical exchanges and guidance development are: 1) the portfolio concept for presenting the case for validation and 2) best practices for reducing the burden of integrated system validations (ISVs) through the application of MSV. The portfolio concept was introduced and briefly outlined in Chapter 6 and a description of what the contents of such a portfolio might be was also described. It is expected that additional development and refinement of the portfolio concept could be useful in further addressing the matter of what is acceptable for achieving reasonable confidence in validation results and conclusions. Capturing best practices that help to reduce the burden of ISV through the application of an MSV would address the practical consideration that resources for the development and validation of designs are limited. It is anticipated that the extent to which the MSV will be implemented will depend largely upon whether it can be implemented without a substantial expansion of the resources required to develop and validate a design. Demonstrating that the costs of early, staged validations can be offset by reduced design or validation efforts elsewhere in the process will be important to encouraging the widespread implementation of MSV.

References

Berntson, K. et al. (2004), "Validation of the Bruce A Unit 3 and 4 SCA – A Case Study", in *Proceedings of the Fourth American Nuclear Society International Topical Meeting on Nuclear Plant Instrumentation, Controls and Human-machine Interface Technology (NPIC & HMIT 2004)*, American Nuclear Society, La Grange, IL.

Davey, E. (2004), "Validation – Experience and Ongoing Challenges", in *Proceedings of Fourth American Nuclear Society International Topical Meeting on Nuclear Plant Instrumentation, Controls and Human-machine Interface Technology (NPIC & HMIT 2004)*, American Nuclear Society, La Grange, IL.

Fuld, R.B. (1997), "V&V: What's the Difference?", *Ergonomics In Design*, Vol. 5(3), Human Factors and Ergonomics Society, Santa Monica, CA.

Green, M. and S. Collier (1999), *Verification and Validation of Human Factors Issues in Control Room Design and Upgrades* (SKI Report 99:10), SKI, Stockholm.

Hanada, S. et al. (2010), "US-APWR Human System Interface System Verification & Validation Program for Digital I&C Design", *American Nuclear Society International Topical Meeting on Nuclear Plant Instrumentation, Controls and Human-machine Interface Technologies (NPIC & HMIT 2017)*, American Nuclear Society, La Grange, IL.

IAEA (2018), *Dependability Assessment of Software for Safety Instrumentation and Control Systems*, IAEA Nuclear Energy Series No. NP-T-3.27, IAEA, Vienna.

IEC (2009), *Nuclear Power Plants – Control Rooms – Design*, IEC 60964, Edition 2.0, IEC, Geneva.

IEC (1995), *Nuclear Power Plants Main Control Rooms – Verification and Validation of Design*, IEC Standard 61771, IEC, Geneva.

ISO/IEC (2005), *Application and Management of the Systems Engineering Process*, ISO 26702/IEEE Std 1220-2005, IEC, Geneva.

ISO (2006), *Ergonomic Design of Control Centres – Part 7: Principles for the Evaluation of Control Centres*, ISO 11064-7:2006, ISO, Geneva.

Koskinen, et al. (2017), "Systems Usability Case in Stepwise Control Room Validation", *Proceedings of 10th American Nuclear Society International Topical Meeting on Nuclear Plant Instrumentation, Controls and Human-machine Interface Technologies (NPIC & HMIT 2017)*, American Nuclear Society, La Grange, IL.

Laarni, J., L. Norros and L. Salo (2017), "Multi-stage approach to control room validation", in *Human Factors Validation of Nuclear Power Plant Control Room Designs and Modifications: Proceedings of the Expert Workshop, Charlotte, United States, 19-21 February 2015*, NEA/CSNI/R(2016)17.

Laarni, J. et al. (2013), "A Stepwise Validation Process for the Main Control Room of Fortum Loviisa Nuclear Power Plant", paper presented at the Enlarged Halden Program Group Meeting, NEA Halden Reactor Project, Halden, Norway.

Malcolm, S., K. Holford and D. Gillard (2000), "HF Verification and Validation Activities: Simulator Based Operational Trials", *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, Human Factors and Ergonomics Society, Santa Monica, CA.

NEA (2017), "Human Factors Validation of Nuclear Power Plant Control Room Designs and Modifications: Proceedings of the Expert Workshop, Charlotte, United States, 19-21 February 2015", NEA/CSNI/R(2016)17 .

NRC (2012), *Human Factors Engineering Program Review Model*, NUREG-0711, Revision 3, NRC, Washington, DC.

NRC (2016), *Standard Review Plan, Chapter 18 – Human Factors Engineering*, NURG-0800, NRC, Washington, DC.

ONR (2013), *The Purpose, Scope, and Content of Safety Cases*, ONR NS-TAST-GD-051, Revision 3, ONR, London.

O'Hara, J. and J. Higgins (2015), *Integrated System Validation: Models, Methods, and Issues*, BNL Technical Report No. 6859-1-2015, Brookhaven National Laboratory, Upton, NY.

Rivere, C. (2015), "Human Factors Engineering Verification and Validation Process of New Nuclear Power Plant Control Room: How to Bridge the Gap from Stepwise V&V to final ISV", *Proceedings of the Ninth American Nuclear Society International Topical Meeting on Nuclear Plant Instrumentation, Controls and Human-machine Interface Technologies (NPIC & HMIT 2015)*, American Nuclear Society, La Grange, IL.

Savioja, P. and L. Norros (2013), "Systems Usability Framework for Evaluating Tools in Safety-Critical Work", *Cognition, Technology, and Work*, Vol. 15 (3), pp. 255-275.

Shin, Y.-C., H.-K. Moon and J.-H. Kim (2006), "Human Factors Engineering Verification and Validation for APR1400 Computerized Control Room", *Proceedings of the Fifth American Nuclear Society International Topical Meeting on Nuclear Plant Instrumentation, Controls and Human-machine Interface Technologies (NPIC & HMIT 2006)*, American Nuclear Society, La Grange, IL.

Appendix A: **Workshop participants**

Invited experts

Joakim Bergroth, Human factors engineering (HFE) expert, VR/AR Lead, Fortum Power and Heat, Finland

Joakim Bergroth is a highly experienced HFE expert at Fortum, which is a leading Nordic power company operating and developing its own and co-owned nuclear power plants (NPPs). His team at Fortum is the Control centres and human-machine interfaces-team (HMI), where he has received hands-on experience of industry best practices in HFE. In the Loviisa NPP automation renewal project, he has been responsible, among other things, for the testing of the safety of HMIs, and configuration management issues. For the past few years, he has also focused on taking the newest digital technologies, such as virtual and augmented reality and interactive 360 videos, into use in the industry. He is a member of the International Electrotechnical Commission (IEC) Subcommittee 45 A standards working group and represents Fortum in the Hambo HFE research group for Nordic NPPs. He holds an M.Sc. in control engineering from Åbo Akademi University in Finland, with minors in industrial computer engineering.

Maren H.R. Eitrheim, Research Scientist, Safety MTO, Industrial Psychology Department at Institute for Energy Technology (IFE), Norway

Maren Eitrheim is a research scientist in the Industrial Psychology Department at the Institute for Energy Technology (IFE) in Halden, Norway. She received her Master's degree in cognitive and biological psychology from the Norwegian University of Science and Technology in 2007. During her ten years at IFE she has conducted human factors simulator experiments in the Halden Man-Machine Laboratory on staffing and human-automation collaboration in future plants, human performance assessment and control room evaluation. She has been involved in projects on resilient operation and maintenance, training and integrated system validation for the nuclear and petroleum industries.

Robert Fuld, Principal Engineer, Human Factors and Operations Group, Plant I&C Organization, Westinghouse Electric Company, LLC., United States

Bob Fuld is a former US Navy reactor operator with 40 years' experience in the operations, maintenance, design, evaluation and licensing of nuclear power plant systems. Mr Fuld is a principal engineer and human factors specialist at Westinghouse Electric Company. He has degrees in both engineering and psychology, and has been certified since 1993 as a Human Factors Professional by the Board of Certification in Professional Ergonomics. He is a past Chair of Subcommittee 5, Human Factors and Control Facilities of the Institute of Electrical and Electronics Engineers (IEEE) Nuclear Power Engineering Committee. His experience includes development of the Korea Next Generation Reactor (KNGR) control room, and validation of the TWICE control room upgrade. In 2015, he was awarded the George Westinghouse Signature Award as one of the members of the team that developed and implemented the AP1000 Integrated System Validation Scenarios.

Brian Green, US Nuclear Regulatory Commission (NRC)

Dr Brian Green is a human factors engineer in the Office of Nuclear Reactor Regulation at the NRC. He is responsible for the assessment of proposed licensing actions related to control room modifications, ex-control room manual actions and other human factors issues at nuclear power plants. Previously, he worked in the Office of New Reactors where he wrote several human factors verification and validation inspection procedures for use in the construction of new plants. Dr Green has a Ph.D. and Master's degree in industrial and systems engineering/human factors from the University of Buffalo. Prior to joining the NRC, he worked as a human factors research assistant at the Research Institute for Safety and Security in Transportation. Dr Green also works as an adjunct professor of psychology at the George Washington University.

Conny O. Holmstrom, Senior Human Factors Specialist and Adviser, Vattenfall AB, Business Area Generation/Nuclear Projects and Services/Engineering

Conny O. Holmstrom is a senior human factors specialist and advisor at Vattenfall AB (governmental body and the largest utility in Sweden). He is a psychologist from Umea University (Sweden) and has devoted quite some time during his career to issues related to system evaluation in terms of test and evaluation, verification and validation in different forms and contexts including both research and development and applied industrial activities. Development and improvement of system evaluation methods have been to a great extent a part of the research work and system evaluations, including for example testing of new functions related to advanced operator support systems or technological improvements in industrial settings. The work has comprised development of a broad spectrum of methods and techniques to be used in "proof-of-principle" tests, different types of user tests, and in more sophisticated large-scale experimental studies or integrated system validations, for example. A handbook was developed a few years ago in which Holmstrom was heavily involved, focusing on how to perform and what methods to be used in evaluations and system testing in applied environments in connection with nuclear new build and/or modernisations of the existing nuclear fleet.

Hanna M.K. Koskinen, Research Scientist, VTT Technical Research Centre of Finland Ltd

Hanna Koskinen is a research scientist at VTT Technical Research Centre of Finland Ltd. Her research focuses on human factors in complex systems and in particular design and development of tools for professional use in safety-critical work context. She holds a Master of Arts in industrial design from the University of Lapland with a minor in work psychology and management from Helsinki University of Technology. During her over ten years at VTT, she has participated in developing design and evaluation methods and conducted a number of control room validations in the NPP context. She has also been involved in projects in other work domains such as remote operation of container cranes and electricity grid operations, as well as being invited as an expert panellist in the Human Dependability Working Group on Space Operations.

Wolfgang Krause, Areva NP HFE Expert, Areva GmbH Germany

Wolfgang Krause studied process engineering at the Nuremberg Institute of Technology Georg Simon Ohm and gained ten years of experience in the engineering of human-system interfaces (HSIs) and control rooms, tightly coupled with the engineering of human factors of nuclear power plants. Wolfgang was the HMI/HF engineer and manager of several Areva projects, including one of the largest modernisations of a plant's complete control centre (OKG2), the HMI for the EPR projects (Olkiluoto OL3, Hinkley Point HPC), and for the first Hualong reactor (Fuqing 5 and 6) conventional HMI. He led, or participated in, as an expert the development of project-specific HF strategies, HF analyses, HF-guided design of both conventional and computerised HMIs and HF verification and validation activities. In his current position, Wolfgang leads a team of 15 HF/HMI engineers, is in charge of developing the HF programme for Angra 3 (Brazil), and a nuclear HF training programme. Wolfgang is member of the NEA Halden Project Programme Group and supports the development of IEC standards (WG8).

Robert Leger, Senior Human Factors Engineer, Candu Energy Inc., Canada

Robert Leger is a senior human factors engineer and the technical lead for the Control Centre and Human Factors Engineering section at Candu Energy Inc. He has a B.Sc. in chemical engineering and mechanical engineering and Ph.D. in engineering physics, specialising in the development of operator support systems. He has worked on several validation projects, ranging from small validation exercises for specific design changes related to station refurbishment activities to preliminary integrated validations for new build projects. He has experience in preforming validations in the station main control rooms, station training simulators and control room mock-ups. He was a member of the subcommittee that developed the Canadian Standards Association (CSA) standard for "Human factors in design for nuclear power plants", CSA N290.12-14.

Nathan Lau, Assistant Professor, the Grado Department of Industrial and Systems Engineering, Virginia Tech, United States

Nathan Lau is Assistant Professor in the Grado Department of Industrial and Systems Engineering at Virginia Polytechnic Institute and State University (Virginia Tech). He received his Bachelor's and Ph.D. degrees from the University of Toronto in 2004 and 2012, respectively. Prior to joining Virginia Tech, he has conducted full scope simulator experiments at the NEA Halden Reactor Project, Halden, Norway, and the Center for Engineering and Research, VA, in the United States. Professor Lau specialises in human-machine interface design and human performance assessment with applications in the process and energy industries.

Luis Rejas Lopez, Control Room and Simulation Manager, Tecnatom S.A., Spain

Luis Rejas Lopez is the current Account Manager of the activities performed in the control room and Simulation Department of Tecnatom, including all HFE activities. He is an Electrical Engineer with a Master's degree from the Polytechnic University of Madrid (Spain). He is also certified as a Senior Reactor Operator of PWRs instructor, and he was teaching in normal, abnormal, emergency and severe accident procedures to main control room crews in the full scope simulator, as well as to plant operators (in the corresponding building) over a period of ten years. He started working in HFE analysis in 1996 in the Lungmen 1 and 2 project (GE) addressing all analysis and design NUREG-0711 elements, first as an engineer with an operating background, and finally as Tecnatom project manager. Since 2008, he has been the former manager of HFE activities in Tecnatom where he developed and designed new Tecnatom Methodologies for addressing all NUREG-0711 elements. Under this department, the complete HFE analysis of South Texas Project (STP-3&4) was performed for Westinghouse, and six more reactors in China (based on US regulation). At the same time, he was the Senior Project Director for design, manufacture, supply and commissioning of the complete main control room (hardware and software) of the cited NPPs where the integrated system validation (ISV) activities were addressed.

Kenji Mashio, Engineering Manager, Mitsubishi Heavy Industries, Ltd. (MHI), Japan

Kenji Mashio has 20 years' experience in NPP HFE and I&C technologies. He has been involved in various NPP HFE and I&C licensing, engineering and construction projects, including Genkai 1 and 2 main control room (MCR) control board replacement (1996-2003, the first control board replacement in Japan) with engineering in charge, Tomari Unit 3 (a new construction with digital I&C and HSI platform in 2003-2005 as HFE/HSI licensing and engineering in charge), Ikata 1 and 2 control board replacement (the first screen-based control board replacement project in 2005 as HFE/HSI licensing in charge), AP1000 DCD Chapter 18 support in WEC (2006), US-APWR DCD Chapter 7, 13 and 18 licensing and engineering in charge (2008-2013), and ATMEA 1 standard design (2014-present). During various projects, he has developed HFE processes and managed HFE implementation.

Alice Salway, Human and Organizational Factors Specialist, Canadian Nuclear Safety Commission, Canada

Alice Salway has worked on design and change management projects in the domains of nuclear power, aviation, transportation, mining, oil and gas, chemical, manufacturing and defence. She is familiar with a range of user-centred methods, structured methods and analysis techniques used for systems design projects. While working in design teams, Alice managed, planned and conducted test, evaluation and validation activities. She was involved in developing military human factors integration/human systems integration approaches and standards in the United Kingdom and Canada, which position validation activities in the systems design process as well as specifying detailed guidance and requirements for validation activities. After a career in human factors engineering that had spanned several decades and continents, Alice joined the Canadian Nuclear Safety Commission as a human factors specialist in 2006. In her current role, she contributes to Canadian standards and regulatory documents, develops approaches and criteria for regulatory inspections and technical assessments, and carries out inspections and assessments of Canadian nuclear licensee's facilities and activities. Alice has a B. Sc. in Ergonomics from Loughborough University of Technology in England and a Ph.D. in cognitive psychology from Aberdeen University in Scotland.

The members of the Working Group on Human and Organisational Factors' Task Group on Validation of Nuclear Power Plant Control Room Designs and Modifications

Per Øivind Braarud, Senior Researcher, NEA Halden Reactor Project/Institute for Energy Technology, Norway

Per Øivind Braarud is a senior researcher at the NEA Halden Reactor Project/Institute for Energy Technology. He has an MSc in psychology from the Norwegian University of Science and Technology (NTNU). He has worked on several human factors integrated system validation (ISV) projects for Swedish modernised reactors. This work has included scenario specifications, specification of human performance measures, and the establishment of applied approaches for the analysis of data and development of conclusions about control room status. He has also worked on several human factors simulator experiments for the Halden Reactor Project (HRP) on topics such as ISV, human reliability analysis (HRA), and teamwork. He is currently project leader for HRP research on ISV focusing on the development of valid human performance measures for ISV applications.

Cecilia De la Garza, Senior Researcher on Ergonomics, Électricité de France, France

Cecilia De la Garza is Senior Researcher at Électricité de France/R&D in the Human and Organizational Factors Group. She has a Doctorate in ergonomics from the Ecole Pratique des Hautes Etudes of Paris, and she specialises in cognitive psychology. She has much experience in ergonomics studies including analysis and solutions-oriented safe design, human factors design and accident prevention in different industrial fields such as nuclear power plants, railways and printing. The last nine years, she has been working in different design projects (new build and modification) and she has contributed to the development of a multidisciplinary approach for the evaluation/validation activities in the framework of an engineering human factors programme applied to the French EPR. Her current work is focused on two main topics: crisis management and new build. She supports different studies in response to the lessons learnt from the Fukushima Daiichi accident. She participates in different human factors studies on simulators to test a new crew concept in extreme situations, with a multidisciplinary approach. She also contributes to the development of new forms of simulation and crisis management training in order to improve the resilience of the sociotechnical system. She is involved in addressing topics such as the ISV, automation and teamwork in a new build design project.

David Desaulniers, Senior Technical Advisor for Human Factors and Human Performance Evaluation, US Nuclear Regulatory Commission, United States

Dr David Desaulniers is a senior level scientist at the United States Nuclear Regulatory Commission (NRC). He currently serves as NRC's Senior Technical Advisor for Human Factors and Human Performance Evaluation, providing expert technical advice on emerging technical and policy issues concerning human performance in nuclear safety. He obtained his doctorate in psychology from Rice University in Houston Texas where he specialised in engineering psychology. During the past 28 years, his work has addressed a wide range of technical and policy issues where there is a nexus between the design and operation of nuclear power plants, human and organisational performance and the protection of public health and safety. Specific past activities include serving as NRC's technical lead for the development of a federal regulation to require fatigue management programmes at all US commercial nuclear power plants and providing human factors technical expertise in agency initiatives concerning severe accident management, crediting manual actions, evaluating the cumulative impact of operator workarounds, and assessing control room conduct of operations. Dr Desaulniers' current work is focused on supporting the NRC's response to the lessons learnt from the nuclear accident at Fukushima Daiichi and the integrated system validation of main control room designs. Dr Desaulniers is also active in industry and international organisations, serving as Chair of the IEEE's Nuclear Power and Energy Committee, Subcommittee 5 (Human Factors, Control Facilities and Reliability) as well as serving as a Vice-Chair of the NEA Working Group on Human and Organisational Factors.

Stephen Fleger, Senior Human Factors Analyst, Nuclear Regulatory Commission, United States

Steve Fleger is a senior human factors analyst in the Office of Nuclear Regulatory Research at the US Nuclear Regulatory Commission. He is a Certified Human Factors Professional (CHFP) from the Board of Certification in professional ergonomics with 38 years of human factors engineering design, analysis and evaluation experience. Before joining the NRC in 2008, Mr Fleger worked in the private sector where he had technical and managerial responsibilities over 70 consulting projects for clients across the commercial and private sectors, including business, industry, the US government and military, and foreign clients in Bulgaria, Japan, Lithuania, Russia and Spain. In 2006, Mr Fleger was nominated and elected as the United States expert to the International Organization for Standardization (ISO) Working Group (WG) 8, Control Centers, by the US TAG to TC159 /SC4, Ergonomics for Human-System Interaction. Mr Fleger served as the Chair of the Institute of Electrical and Electronics Engineers (IEEE) Nuclear Power Engineering Committee Subcommittee 5 (SC5) for six years. SC5 is responsible for developing human factors engineering consensus standards for nuclear facility control centres. In this capacity, he led the effort to develop and publish IEEE Standard 1786™-2011, IEEE Guide for Human Factors Applications of Computerized Operating Procedure Systems (COPS) at Nuclear Power Generating Stations and Other Nuclear Facilities. Mr Fleger is a Past Chair of IEEE's Nuclear Power Engineering Committee, the Secretary of SC5, and the Chair of WG 5.2, Interface Design.

Cyril Rivere, Human Factors Specialist*, Areva, France

Cyril Rivere is a human factors specialist, with a Master and Ph.D. in Ergonomics, completing a biology and physiology educational background. Prior to working for Areva, he worked in a large company specialised in high performance materials and packaging manufacturing, where he developed methods for ergonomics of product applied to packaging design, favouring ergonomics and end-user integration in the design process. Since 2009, Cyril is specialised in industrial complex systems addressing Human and Organizational Factors issues as Human Factors Engineering Specialist for Areva NP Company, where he is in charge of integrating the human factors discipline within the Engineering and Projects organisation with a focus on large nuclear power plant new build projects. In this position, Cyril pilots (from an engineering and project management standpoint) and implements human factors principles, methods and requirements for several NPP projects, with a large part dealing with human factors preliminary analyses (FRA/FA, TA and OER) and Control Center, Control Room and HSI design. In addition, he developed for these projects the entire verification and validation approach, and is currently in charge of leading the integrated system validation process for one of them. As Areva's Human Factors Specialist, Cyril is in charge of training activities for engineers as well as customers and safety authorities, and he also provides support in the development of R&D projects.

Jari Laarni, Principal Scientist, VTT Technical Research Centre of Finland

Jari Laarni is Principal Scientist at the Systems Research Centre of VTT Research Centre of Finland. He has a Ph.D. and Master's degree in psychology from the University of Helsinki, Finland. He is specialised in the areas of cognitive psychology, cognitive science, human factors, ergonomics, user-centred design, systems usability, human well-being and stress, and he has participated in several national and international research projects on these topics. He has also been involved in several projects in Finland concerning verification and validation (V&V) of NPP control room systems.

Dina Notte, Human Factors Expert*, ERGODIN Consulting, Belgium

Dina Notte has an industrial psychologist and ergonomist education. She has founded ERGODIN consulting company and has worked for 35 years in the design of computerised control rooms and HSI in high-risk industrial processes like nuclear power plants, petrochemical sites, railway traffic controls, steel industry and robotics in surgery and telemedicine. Dina is has experience in the management of HF integration in long-term and complex projects encompassing technical challenges (i.e. artificial intelligence, robotics, high automation and computerisation) and human reliability issues. During these projects, she had to build-up sophisticated HSI validation and verification methods and experimental protocols (i.e. Wizard of Oz techniques, Satellite Communication Simulation) based upon human performance metrics (i.e. cognitive workload assessment, cognitive walkthrough, team work evaluation). Dina has been a member of the Human Factors and Ergonomics Society (HFES) since 1985, as well as the Société d'ergonomie de langue française (SELF) since 1984. She is an HF expert for European Commission DG III, DG XII and DG XIII. She has been general secretary of the French Ergonomic Society for six years, and has been a Certified European Ergonomist since 1995.

John O'Hara, Senior Scientist, Brookhaven National Laboratory, United States

Dr John O'Hara is a senior scientist at Brookhaven National Laboratory and its Human Factors Research Manager. His research programmes address the effects of advanced technology on individual and crew performance in complex systems. Specific programmes address: 1) human factors engineering methods and tools; 2) the development of human factors design guidance for advanced systems including alarms, information systems, computer-based procedures and controls; 3) the role of cognitive factors, such as attention, situation assessment and workload in complex system operation and human error; and 4) evaluation methods of individual and integrated human-system performance. John's research has focused on many types of industrial systems, including: nuclear power, space, aviation, robotics, maritime and homeland security. He has also performed numerous safety evaluations and design reviews of various types of complex systems, including nuclear power plants and NASA control centres. John is a Certified Human Factors Professional; Fellow of the Human Factors and Ergonomic Society; and Past Chair of American Nuclear Society's (ANS's) Human Factors, Instrumentation and Control Division (HFICD).

Paula Savioja-Kangasluoma, Senior Inspector, STUK, Radiation and Nuclear Safety Authority, Finland

Paula Savioja-Kangasluoma is a senior inspector at the Finnish Radiation and Nuclear Safety Authority STUK. She has a Doctor of Technology degree from Aalto University and a Master's degree in engineering from Helsinki University of Technology. Previously, she worked for more than 15 years at VTT Technical Research Centre of Finland conducting and managing human factors research work in various safety-critical domains. The majority of her own research work concerned development of NPP operator work and control room design. Her dissertation, "Evaluation of Systems Usability in Complex Work", developed the practices of conducting control room evaluation studies in realistic settings. In her current position in the Operational Safety Office of STUK, she is responsible for the oversight of human factors engineering processes and practices of operating NPPs and NPPS under-construction in Finland.

* Task group members contributing to the development of the paper but not present at workshop.

Appendix B: **Workshop agenda**

Experts' Workshop on Multi-Stage Validation of Nuclear Power Plant Control Room Designs and Modifications

Hyatt Regency – San Francisco – Garden Room A, 2017, Thursday 8 June

Opening Remarks and Presentations

- David Desaulniers, US Nuclear Regulatory Commission – Welcome, Meeting Objectives, and Overview of Workshop Agenda.
- Yeonhee Hah, Nuclear Energy Agency, Human Aspects of Nuclear Safety (HANS) Division – Perspectives from the Head of HANS
- Monica Haage, Nuclear Energy Agency, Division of Human Aspects of Nuclear Safety – Overview of the Working Group on Human and Organisational Factors

Objective 1: Gaining Common Understanding and Alignment on the Defining and Desirable Characteristics of a multi-stage validation (MSV)

- Overview of MSV defining and desirable characteristics (Chapter 3), *David Desaulniers, US Nuclear Regulatory Commission*
- Expert commentary presentations on MSV defining and desirable characteristics – *Invited Experts*
- Task group queries experts/experts query task group *(all)*
- Small Group* Discussion – Defining Characteristics
- Small Group Discussion – Desirable Characteristics
- Small group reports (3)
- Discussion on common themes and differences *(all)*

  Facilitators: Steve Fleger (US NRC) and Paula Savioja-Kangasluoma (STUK)

Experts' Workshop on Multi-Stage Validation of Nuclear Power Plant Control Room Designs and Modifications

Hyatt Regency – San Francisco – Garden Room A, 2017,Friday 9 June

Day 1 Summary – Implications for the working group report/Days 2 and 3

Jari Laarni, VTT Research Centre of Finland

Objective 2: Identify and discuss methods for conducting staged validations that optimise the building of cumulative evidence

- Overview of an example MSV (Chapter 4), *John O'Hara, Brookhaven National Laboratory*
- Expert commentary presentations on an example MSV and methods *(invited experts)*
- Task group queries experts/experts query task group *(all)*
- Small Group Discussion – Staged validation methods and practices, Focus: HFE Planning and Analysis, Requirements Specification, Concept Design
- Small Group Discussion – Staged validation methods and practices
- Focus: Subsystem Design, Integrated system, Deployment/Operations, Design Modification
- Small Group Reports (3)
- Discussion on common themes and differences *(all)*

  Facilitators: Steve Fleger (US NRC) and Paula Savioja-Kangasluoma (STUK)

Experts' Workshop on Multi-Stage Validation of Nuclear Power Plant Control Room Designs and Modifications

Hyatt Regency – San Francisco – Garden Room A, 2017, Saturday 10 June

Day 2 Summary – Implications for the working group report/Day 3

Cecilia De la Garza, Électricité de France

Objective 3: Identify best practices for creating the MSV portfolio/safety case

- Overview of Integrating Results Across Stages and Validation Documentation (Chapter 5), *Per Oivind Braarud, NEA Halden Reactor Project*
- Expert commentary presentations on Integrating Results Across Stages and Validation Documentation (*invited experts*)
- Task group queries experts/experts query task group
- Small Group Discussion – Best Practices for creating the MSV portfolio/safety case
- Small Group Reports (3)
- Discussion on common themes and differences (all)

  Facilitators: Steve Fleger (US NRC) and Paula Savioja-Kangasluoma (STUK)

Meeting summation and closing remarks (D. Desaulniers)

* For the small group discussions, workshop participants (invited experts and task group members) were divided into three groups of approximately seven individuals.

NEA PUBLICATIONS AND INFORMATION

The full catalogue of publications is available online at www.oecd-nea.org/pub.

In addition to basic information on the Agency and its work programme, the NEA website offers free downloads of hundreds of technical and policy-oriented reports. The professional journal of the Agency, NEA News – featuring articles on the latest nuclear energy issues – is available online at www.oecd-nea.org/nea-news.

An NEA monthly electronic bulletin is distributed free of charge to subscribers, providing updates of new results, events and publications. Sign up at www.oecd-nea.org/bulletin.

Visit us on Facebook at www.facebook.com/OECDNuclearEnergyAgency or follow us on Twitter @OECD_NEA.

OECD/NEA PUBLISHING, 2 rue André-Pascal, 75775 PARIS CEDEX 16

Multi-Stage Validation of Nuclear Power Plant Control Room Designs and Modifications

A mature and well-guided multi-stage approach to the validation of nuclear power plant control room designs has the potential to reduce the risks involved in the design process. Such an approach can also increase the effectiveness of, and efficiencies in, the validation process, as well as overall confidence in the results. This relatively new concept of multi-stage validation has yet to be defined in the technical literature, and thus the report describes the approach and the rationale for validating systems through a series of successive, co-ordinated validation activities. The scope of application of multi-scale validation addressed in the context of this report includes aspects related to both the human factors engineering of new nuclear power plant main control room designs and modifications to existing control room designs. The objective is to provide a common reference for future dialogue, research and development concerning the multi-stage validation approach, and ultimately to support the safe operation of nuclear power plants worldwide.

Nuclear Energy Agency (NEA)
46, quai Alphonse Le Gallo
92100 Boulogne-Billancourt, France
Tel.: +33 (0)1 73 21 28 19
nea@oecd-nea.org www.oecd-nea.org

NEA No. 7466