SYSTEMS USABILITY CASE IN STEPWISE CONTROL ROOM VALIDATION

Hanna Koskinen, Jari Laarni, Marja Liinasuo
VTT Technical Research Centre of Finland
Vuorimiehentie 3, Espoo, P.O. Box 1000, FIN-02044 VTT, Finland
firstname.lastname@vtt.fi

Leena Norros
University of Helsinki
PL 3 (Fabianinkatu 33), 00014 Helsingin yliopisto
firstname.lastname@elisanet.fi

Paula Savioja
Radiation and Nuclear Safety Authority (STUK)
Laippatie 4, Helsinki, P.O.Box 14, 00881 Helsinki, Finland
firstname.lastname@stuk.fi

ABSTRACT

We present a Systems Usability Case (SUC) approach enabling a requirement-based human factors evaluation of complex technical systems. The approach is especially suitable for stepwise verification and validation (V&V) of nuclear power plant (NPP) control room (CR) systems. A SUC is based on the Safety Case approach and on the Systems Usability (SU) construct. A series of V&V test activities carried throughout the design process and constructed according to SUC enables us to monitor how evaluation evidence is aggregated over variety of V&V steps and how the design solution is maturing towards a tool of a good quality and usability. The paper demonstrates an application of the SUC approach to real data from a stepwise CR validation. The results suggest that SUC has some clear advantages. It makes it easier to conduct the V&V activities in a more systematic fashion and it makes the reasoning process more explicit and transparent. Moreover, it enables building a longitudinal view of the progress of the design process. Most importantly, constructing the SUC enables monitoring of the fulfilment of the requirements from the human factors (i.e., SU) perspective.

Key Words: systems usability case, stepwise V&V, control room systems

1 INTRODUCTION

When people are talking about complex technical systems, a nuclear power plant (NPP) has been typically presented as an ideal example. Controlling this kind of complex system (or system of systems) is a challenging enterprise. Furthermore, the lifecycle of NPP is often very long, and the different parts of the systems are actively developed and upgraded during the plant's operational lifecycle. For example, CR systems may be upgraded as a response to technological advancements or changes in the operational and safety demands. In many cases, during the system lifecycle, changes and upgrades are also required to the CR systems and human-system interfaces (HSI). The extent of these changes may vary from just upgrading the computer displays to newer ones to fully digitalizing the CR systems and HSIs in connection of a larger automation modernization project. Despite the extent of the changes, human factors engineering (HFE) should be considered as a necessary task to accomplish and, thus, an integral part of the NPP lifecycle activities.

CR evaluation, i.e., verification and validation (V&V), is a critical HFE activity in ensuring a proper functioning of the CR systems and HSIs. Systematic efforts are needed to gather and document human factors data at different phases of the plant's operational life and during the design of different CR systems and HSI upgrades. Carrying out a comprehensive evaluation of the CR systems and HSIs, however, involve several methodological challenges. First, each CR with its respective HSIs is a unique entity, and no reference system that could be directly used as a baseline when assessing the system's usability may be found. The implementation of an upgrade project may also be a very long and time-consuming activity and result an abundance of information and data to be handled and managed. Furthermore, it is often not operatively possible or economically feasible to do all the required changes at once; instead, the upgrades are implemented in several stages. Consequently, also the human factors efforts and the V&V activities need to be planned and organized in a stepwise manner. This means that since each stage has a dedicated set of V&V activities and evaluations, there are new kinds of management and coordination challenges between project stages. For example, how should the human factors data produced throughout the upgrade project be organized to be not only useful in making the conclusion of the acceptability of the system in one particular stage but also produce a more comprehensive, longitudinal understanding of the development of the usability of the system? To manage these challenges and ensure an appropriate HFE perspective, more agile, lean and continuous knowledge management approaches are required. We present a new methodological approach – that is, the Systems Usability Case (SUC) – enabling a requirement-based human factors evaluation of complex technical systems such as the CR systems and HSIs of NPPs. A SUC is based on the Safety Case approach and on the Systems Usability (SU) construct. SUC is considered especially suitable for stepwise V&V of CR systems. SUC provides a useful alternative approach to CR V&V as it does not require extensive benchmarking studies in order to define the acceptance criteria; neither does it involve extensive expert evaluation.

There are several benefits in applying case-based approach like SUC in the stepwise evaluation of CR systems and HSIs. First, it is beneficial in the management and systematization of human factors evidence. Professional and comprehensive knowledge management enables for example transparency and better monitoring the proceeding of the project. It also creates a better foundation for information integration and comprehension. The case-based approach may also help in focusing and giving a timely and an appropriate weight on critical aspects of the system. Furthermore, the approach may provide continuous support for ongoing iterative design of CR systems by producing regular feedback to design. Finally, by accumulating validation evidence over test activities a more thorough evaluation of the CR systems is possible.

In this paper, we first discuss the multi-stage validation in CR design process. After which, the safety case-based SUC approach to CR systems and HSIs V&V is presented in more detail. The practical application of the SUC is demonstrated with reference to a real life CR modernization project. In the final section, we summarize the benefits that SUC may hold and discuss its methodological limitations and the development needs that may direct our future research.

1.1 SUB-SYSTEM VALIDATION IN CR DESIGN PROCESS

Traditionally, one extensive and comprehensive validation effort (i.e., integrated system validation ISV) is made in the end of any major change of CR systems and HSIs. However, often it is sensible and practically feasible to carry out the implementation of CR renewals in a stepwise manner. For example, in a full-scale automation modernization project, reactor and turbine automation may be upgraded in successive stages. Because of the extent of the design task and the large scope of renewed systems, also the V&V activities of the new systems may proceed in a stepwise manner, starting from the evaluation of sub-systems functionality and usability towards the validation of whole integrated CR system.

In order to better respond to the needs of large-scale upgrade projects, an evaluation approach called sub-system validation (SSVs) has been introduced [1] (Figure 1). The design and development work is iterative by its nature and inherently always includes an evaluation of the produced design solutions.

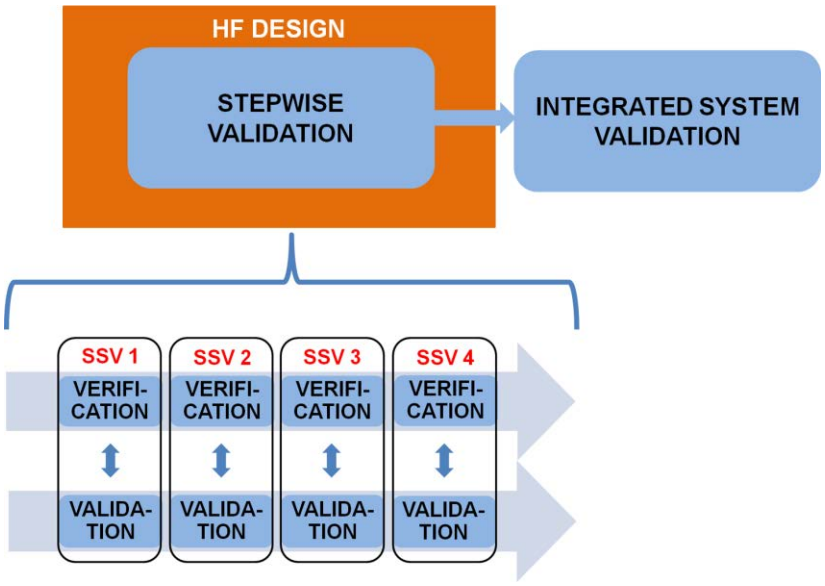

Figure 1. Stepwise validation in CR design (see [1]). The arrows indicate the time line of the SSV activities.

However, a more formal, external V&V of the proposed systems is also required in upgrade projects. Irrespective of whether being design internal or the more formal V&V, the human factors evaluations should aim at tracing and localizing design flaws and places for improvements. Acting upon and solving possible design problems as early as possible saves time and money and may contribute greatly to achieving successful design. In general, SSVs may be useful not only for evaluation and assessment purposes but also for generation of design relevant information that may further successful maturation of the design solution.

Many viewpoints have to be considered when performing SSV as a part of stepwise CR system and HSIs V&V. For example, the different stages of the design process may set different demands on the V&V process, and different timeframes are needed in the design of different parts of the system. Furthermore, there are different HFE focus areas, such as user interface and procedure design, simulator facilities and training of operative personnel that are greatly affected by the upgrade project. All these aspects should be one way or the other considered also when planning and implementing V&V activities for CR systems and HSIs.

2 SYSTEMS USABILITY CASE METHODOLOGY

2.1 Safety Case

A safety case is a definitive requirement in many safety standards, and therefore safety cases are required to be produced in many safety-critical domains such as rail transport and military, off-shore and nuclear industries. According to one definition, a safety case is "*a documented body of evidence that provides a convincing and valid argument that a system is adequately safe for a given application in a given environment*" [2]. The idea of a safety case is to gather safety-related information into one document that is usable during the system's lifecycle to demonstrate the safety of the system. The safety case provides a frame within which the safety related information may be documented and organized in a structured way. Furthermore, in the safety case the abstraction level and the interconnections between pieces of information may be taken account and made explicit. Safety cases are built and structured based on three main elements: claims, evidence and arguments. *Claim* is entity that express a property of the system. *Evidence* is data about the system's ability to support safety, and it is used as the basis of making safety argument. *Arguments* are the links that connect the pieces of evidence to the claims.

2.2 Systems Usability Case Definition

Case-based approach and documentation may also be beneficial in the context of usability evaluation in order to better manage and organize the human factors information regards the usability of CR systems and HSIs. Given the specific demands that are set for usability in the design of complex and unique CR systems, there is a great need for a clear methodology to take into account the versatile nature of usability evaluations. As a response to this, we have used the basic idea and structure of the safety case methodology (i.e., make an explicit set of claims, produce evidence as basis for making arguments) and applied it to building a Systems Usability Case. However, in SUC we have modified and extended the safety case by two ways: Firstly, in addition to the positive and supportive evidence, i.e., human engineering consistency (HEC), from usability evaluation point of view it is also relevant to take into account the negative evidence. In SUC, the design deficiencies that are identified in the evaluation process are categorized as negative evidence and expressed in a form of human engineering discrepancies (HEDs). HEDs may be deviations from optimal operator performance, defined requirements and design conventions. Secondly, instead of just generating a documented final statement/ description of the good performance of the system to be used during its operation, SUC aims at producing information relevant to the design process, that is, it provides guidance and feedback for furthering the design solution.

Taking into account the above-mentioned elaborations, a SUC may be defined as aiming at "*creating an accumulated documented body of evidence throughout the design that provides a convincing and valid argument of the degree of usability of a system for a given application in a given environment*" [3]. The usability-focused case may enable a requirement-based human factors evaluation of CR systems and HSIs. In the Systems Usability construct, the targeted quality of an appropriate technology is comprehended from human factors point of view. The SU provides a contextually defined human factors requirement towards which the design solution should be steered, and which the end product should fulfill. SU expresses "*the capability of a technology to support fulfilment of the work demands so that the objectives of the activity are met, and the technology has the capability to support the three theory-based general tool functions, the instrumental, psychological, and communicative functions*" [4, 5]. CR systems and HSIs of a good quality (i.e., with high SU) provide leverage for the operating personnel to act in a reliable and safe manner. Thus, they should support resilience of a system and lead to its overall safety.

3 CONSTRUCTING A SYSTEMS USABILITY CASE

Because a huge amount of data is produced and collected during the SSV tests, systematic methods are needed for the accumulation and systematization of validation evidence and for drawing conclusions from the evidence. As said, a case-based approach seems particularly suitable when the system to be evaluated is unique and comparison to other systems is difficult. One of the main aims of establishing a SUC is to bring to the front the arguments and evidence for safety in such a way that the argumentation is convincing, and the fulfilment of regulatory requirements can be evaluated. Another aim of the SUC is to make decisions about safety traceable throughout the lifecycle of a product.

Figure 2 below demonstrates how the validation evidence is aggregated and design solutions are maturated over V&V test activities. It also demonstrated how the individual SSV test activities are interrelated. There is a progression of fulfilment of human factors requirements through the time of validation. Some of the HEDs are resolved in one stage, but the revised design solutions have to be retested in the next stage. In addition, requirements may change or become more precise, and new requirements may be identified during the validation process. However, the idea is that at in the end of the V&V process all the HEDs are resolved and, new requirements do not emerge any longer. Figure 2 also indicates that SUC provides support both for the continuous evaluation of the design solutions and for the independent validation of the CR systems. As indicated by the Figure 2, SUC development is divided into two main efforts: the first part of the case (i.e., goal structure) is established before the accomplishment of validation test activities, the latter part (i.e., claim structure) is established after the implementation of the validation

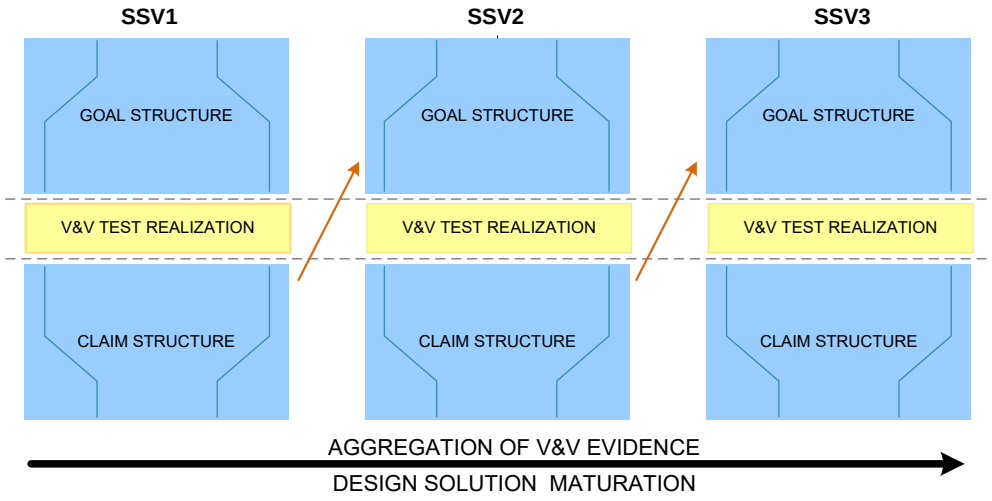

Figure 2. SUC development process illustrating the aggregation of V&V evidence and maturation of the design solution over SSV tests.

test [6, 7]. These two parts are described in more detail below.

3.1 Basic structure of a SUC

As said, a SUC consists of two main parts, a goal structure and a claim structure part (Figure 3). The goal structure part is generated before the actual V&V test activities. It provides the reference base for the V&V test activities. The high-level *acceptance goal* describes the ultimate objective of V&V, and it is expressed in terms of avoidance of human error. The general idea is that the acceptance goal is divided into several sub-level goals, i.e., into *SU* and *plant-specific requirements*. For each requirement, a specific *acceptance criterion*/a set of criteria can be derived. Acceptance criteria make possible to determine whether and to what degree the design conforms to the requirements. Finally, an operational *test condition* is determined for each of these criteria referring to a test case where a particular criterion may be assessed.

In Figure 3, the colored shapes illustrate individual items or statements in the framework. If we move from the top down, the acceptance goal is first connected to the nine general theory-driven SU requirements, which, in turn, are linked to a set of plant-specific requirements. These requirements are then connected to the acceptance criteria and finally the acceptance criteria are linked to specified test conditions. The actual validation test realization is illustrated with a horizontal yellow text box, under which the items of evidence are depicted.

Acceptance criteria that explicitly argue specific claims about the design are derived from the above-mentioned requirements, and their fulfilment is then tested in validation test scenarios by a set of performance measures. Both performance measures and operational conditions/scenarios available set constraints for the specification of acceptance criteria (e.g., for their accuracy): Acceptance criteria have to be defined in a way that makes possible to measure them by existing performance measures and also takes into account the details of the selected operational conditions/scenarios.

The claim structure part (see lower part of the Figure 3), a kind of mirror image of the goal structure part, enables case-based structuring of V&V test results. To be precise, creating a documented body of evidence that provides a valid argument of the degree of usability of the system under consideration. An item of *evidence* is a description of operator performance in the context of a particular operational condition. For each test condition, at least one item of evidence is produced. Items of evidence may be either positive or negative from the point of view of the design depending on whether the corresponding acceptance

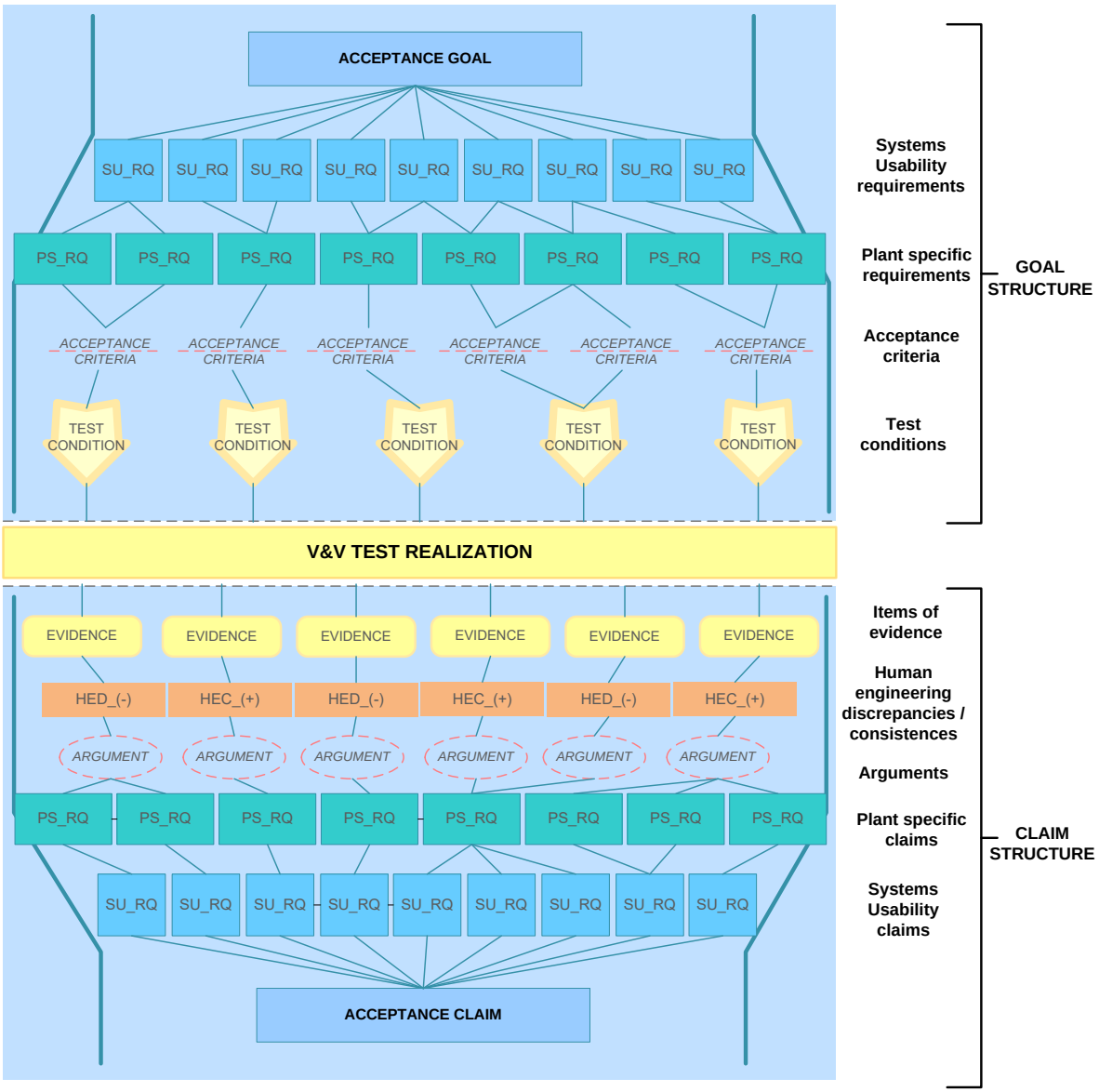

Figure 3. General SUC framework including goal structure and claim structure parts.

criterion is met or not. Positive evidence, that is, a set of HECs, is in conformity with the criterion, whereas, if the criterion is not met, a HED is introduced describing the problem that has been identified.

Argumentation is one of the key operations in constructing of a SUC. The question is how the conclusions are reached through reasoning, in this case, how the evidence approves or rejects the claim. Each HED is considered individually and *an argument* is formulated for the following three questions: 1) Why is this HED important; 2) how does it affect operating activity; 3) what reasoning will show that the evidence either approves or rejects the claim. Arguments can be categorized into a small set of classes. For example, in one SSV test, the arguments were categorized into the following four classes: 1) Arguments drawing on the quality of interface design; 2) arguments drawing on complicated operating activity and increased task load; 3) arguments drawing on errors or possibility of errors; 4) arguments drawing on general features of operational concept.

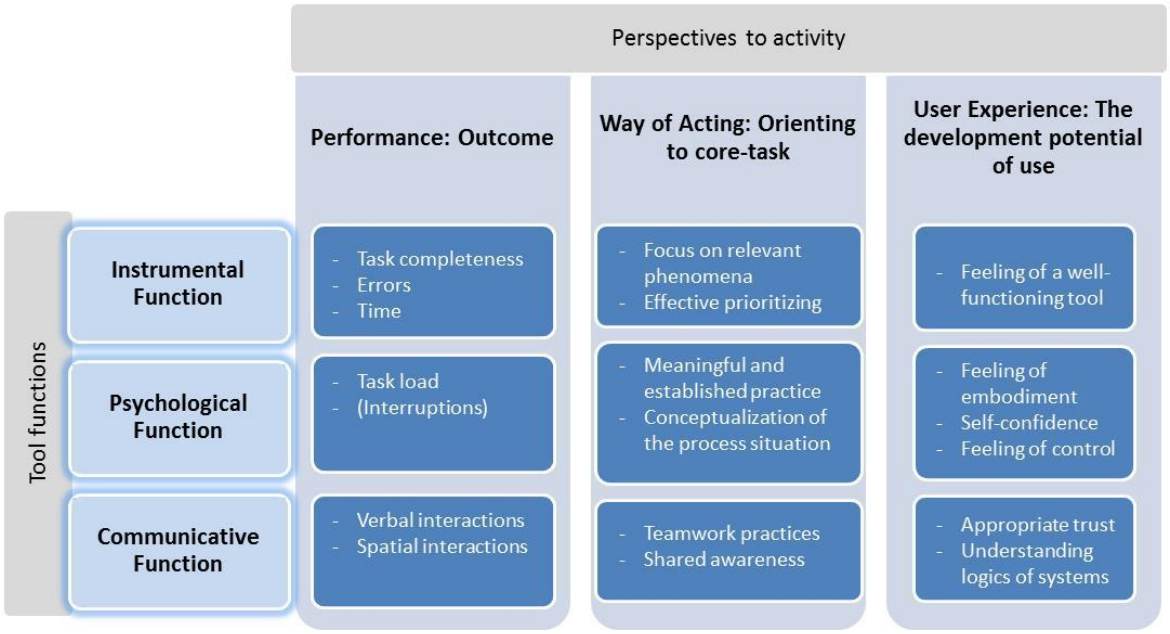

Figure 4. Systems Usability framework for the identification performance measures [4].

In order to form the complete SUC, the final task is to connect the arguments to *the plant-specific* and *SU claims*, which are shown at the bottom part of the SUC framework in Figure 3. The *acceptance claim* shown at the very bottom expresses the ultimate desirable property of the system at which the design process is aiming.

To repeat, if we move from the top down in the claim structure part of Figure 3, beginning from the identified HECs/HEDs, the HECs/HEDs are connected to the arguments; below them we have the plant-specific claims and the SU claims, and finally at the very bottom the general acceptance claim. The idea is that high-level SU claims are guiding the reasoning, and this claim (requirement)-argument-evidence structure is used in building a SUC by using SSV test results.

SUC provides a requirements-based approach to system validation, in which plant-specific requirements are systematically used as a reference in the assessment of acceptability of the CR solutions. V&V of CR systems and HSIs is considered as an activity in which a general claim of system safety is further divided into design requirements and theoretically derived human factors requirements. Plant-specific requirements provide one reference for evaluation; another reference is provided by more theoretically derived human factors requirements that are based on the SU construct and standards and guidelines. Nine categories of the SU framework with some typical indicators concerning NPP operator work are depicted in Figure 4.

3.2 Demonstration

Next, we will present a simplified real-life example to illustrate the application of the SUC approach. The presented example is related to a validation activity targeted to safety HSIs and new emergency operating procedures (EOPs) introduced in the connection of one modernization project. In Figure 5, a goal structure of a SUC concerning one SSV test activity of the real-life modernization-project example case is presented.

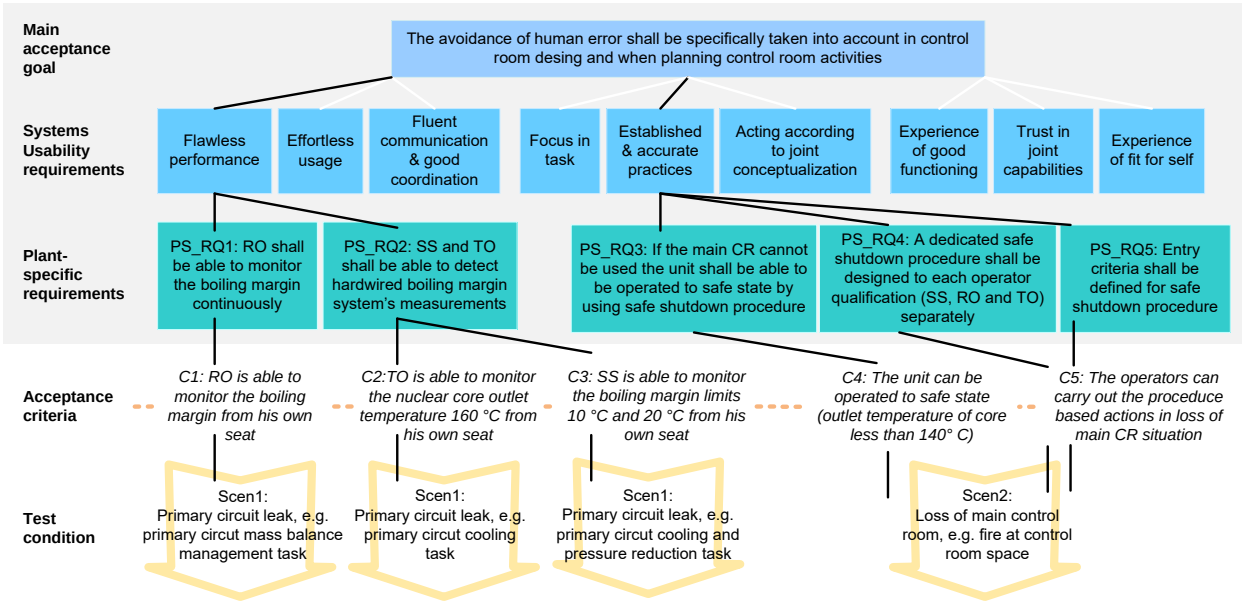

Figure 5. Example of a goal structure part of a SUC in a CR modernization project. The illustrated example is limited to two subset of requirements concerning two individual design solutions (i.e., HSI and EOP solutions).

The main acceptance goal and the SU requirements are common to all SSVs (see the two upper rows in the Figure 5), but the tabulated plant-specific requirements are specific to a particular SSV test. There are dozens of relevant plant-specific requirements, however, only some of them are demonstrated here and displayed in Figure 5. The leftmost two plant-specific requirements (PS_RQ1 and PS_RQ2) belong together, as well as the three rightmost requirements (PS_RQ3, PS_RQ4 and PS_RQ5). The two leftmost requirements concern a specific safety HSI element. The three rightmost requirements concern the operational concept and a specific type of new EOPs.

The acceptance criteria are described as precisely as it is reasonable and possible to do. Several acceptance criteria can be created to one plant-specific requirement in order to improve the reliability of the assessment. For example, in Figure 5, two acceptance criteria (C2 and C3) are linked to PS_RQ2, but only one (C1, C4 and C5) to the other four requirements. It can also be seen that the acceptance criteria C5 is common to PS_RQ4 and PS_RQ5. The procedure in which acceptance criteria are created and linked to requirements is also important in weighting the feasibility and functionality of requirements. For example, if the requirements are too general, it is impossible to verify them by a reasonable set of criteria. On the other hand, the requirements can also be too specific so that it is difficult to generate relevant acceptance criteria to them. Below the acceptance criteria, there are a set of test conditions, which specify operational conditions, functions or tasks in which the five acceptance criteria can be assessed. Typically, test conditions are designed in such way that a multitude of acceptance criteria can be tested in a single test condition. For example, according to Figure 5, two acceptance criteria (C4 and C5) are tested in one scenario (Scen2).

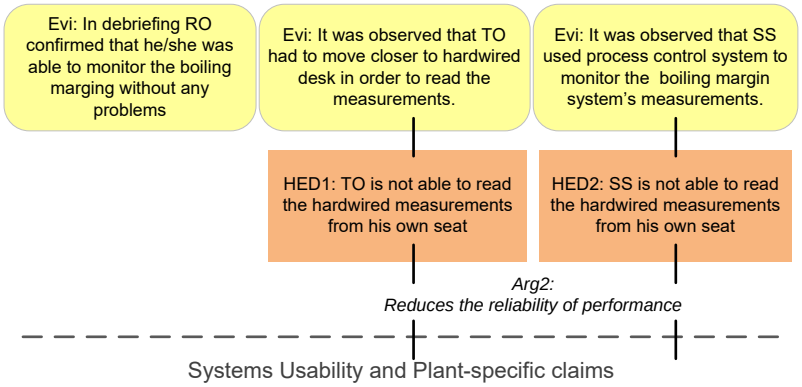

Figure 6. Demonstration of Evidence-HED-Argument linkages to claims (requirements) concerning the HSI solution in our example case. Only the two HEDs are presented.

With regard to a specific SSV test, a part of the requirements is typically met, the latter part is not. It is the task of the design organization to make a decision of what should be done for the non-fulfilled claims (requirements) and HEDs connected to them. The classification of HEDs according their safety-criticality and importance is based on an expert elicitation process. All the HEDs are included in the SUC, but their criticality and importance are taken into account. Arguments play a mediating role between HEDs and claims (requirements). Sometimes, a particular HED does not cause any actions; in most cases, the HED cannot be ignored, but instead it must be settled through redesign, or it must be taken into consideration in operator training or in procedure design. In our example case (Figure 6 above), the operators can live with the HED 1 and 2, because there are other sources of information that can be used to obtain the same information.

For HEDs 3, 4 and 5 (Figure 7), a new requirement emerged (see the plant-specific claims row in Figure 8 next page) that has to be considered in procedure design and evaluated in the next SSV test activity or in the ISV realized in the end of the modernization project. With the SU claims, the critical question is whether they are threatened in that particular condition, and how much positive and negative evidence is piled up in support or in opposition to them. In order to make the SUC complete, the main acceptance claim is depicted (Figure 8), and, as can be seen, it is the same as the acceptance goal depicted on the topmost row in the goal structure (Figure 5).

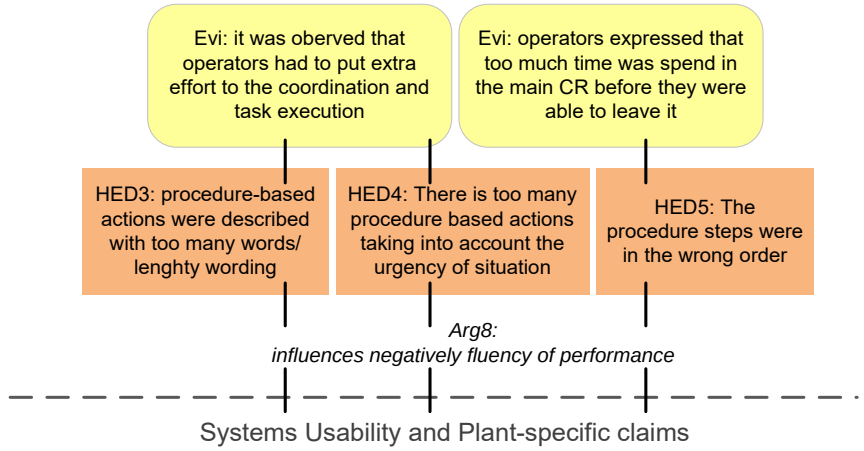

Figure 7. Demonstration of Evidence-HED-Argument linkages to claims (requirements) concerning the EOP solution in our example case. Only the HEDs (i.e., negative evidence) are presented.

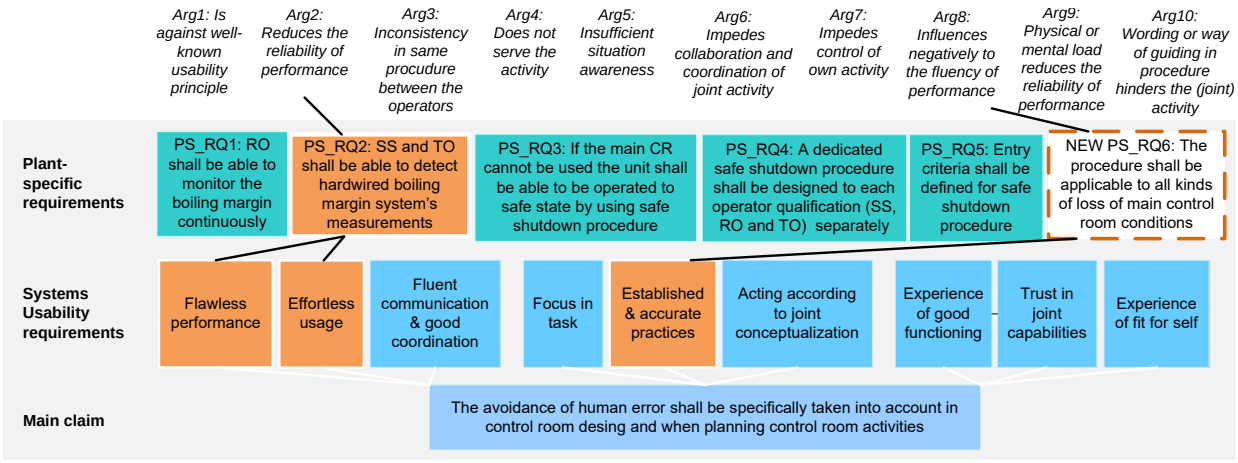

Figure 8. Claim structure part of the SUC. The illustrated example is limited to two subset of requirements concerning two individual design solutions (i.e., HSI and EOP solutions).

4 CONCLUSIONS

Because a lot of data is collected throughout the life-cycle of the plant, systematic methods are needed for the accumulation and systematization of validation evidence and drawing conclusions from the evidence. During the development of the SSV approach, it was reasoned that a case-based approach that is, SUC is particularly suitable approach when the system to be evaluated is unique and comparison to other systems is difficult. It also supports formative evaluation, in which the interest is to steer the development of the system by successive evaluations, and nevertheless remain independent of the design process itself. Notation systems such as the one shown above can be used in the systematization of requirements, arguments and validation evidence.

To establish a complete SUC for a particular SSV test activity is a huge effort, therefore it is not reasonable to apply it in a complete and rigid way. We have established a SUC for real cases, but so far we have not applied it throughout the design process. Therefore, a total picture of its applicability has not yet been reached.

What is the benefit of SUC? It is apparent that constructing a SUC helps in the systematic execution of V&V tests and in systematization of test results. SUC also urges us to think about critical validation questions beforehand. Furthermore, in SUC the chain of reasoning based on the evidence is made explicit and transparent, and it helps us to draw attention to the main problems and important questions. Finally, utilizing the theory-driven SU requirements make it possible to evaluate the scope and coverage of design requirements, monitor the fulfilment of requirements in a longitudinal manner, and assess the scope of plant-specific requirements in relation to the theory-driven SU requirements.

We have deployed the SUC approach in the aggregation of validation information to improve the design and systematize the validation process. However, it is also possible that all human factors related safety justification data could be arranged in a so-called human factors case (HFC) so that a compilation of claims concerning various aspects of HFE of a NPP operation could be organized to constitute the claim base for a HFC. This compilation could include safety claims about various HF issues, e.g., in management, operations, training, HRA and maintenance. Evidence for these claims could be collected with various methods, and the argumentation, why the evidence demonstrates the fulfilling of the claim would be formulated in a similar fashion as in SUC [8].

5 ACKNOWLEDGMENTS

We would like to acknowledge Fortum designers for sharing their valuable experiences on the development and use of the SUC approach.

6 REFERENCES

1. J. Laarni, H. Karvonen, H. Koskinen, M. Liinasuo, L. Norros, P. Savioja, L. Salo, A-M, Laakso, and M. Lehtonen, "A stepwise validation process for the main control room of Fortum Loviisa nuclear power plant," in *Proceedings of the 37th Enlarged Halden Programme Group Meeting, Storefjell*, Norway, March 10-15, (2013).
2. P. Bishop and R. A. Bloomfield, "Methodology for Safety Case Development," in *Proceedings of in Safety-Critical Systems Symposium*. Birmingham, UK, (1998).
3. M. Liinasuo and L. Norros, "Usability Case - integrating usability evaluations in design," in *Proceedings of in COST-MAUSE Workshop on Downstream Utility.* Toulouse, France, (2007).
4. P. Savioja, *Evaluating Systems Usability in Complex Systems. Development of a Systemic Usability Concept to Benefit Control Room Design*. Dissertation. Espoo, VTT, (2014).
5. P. Savioja and L. Norros, "Systems usability - promoting core-task oriented work practices", in E. Law et al. (Eds.), *Maturing Usability: Quality in Software, Interaction and Value,* London, Springer, pp. 123-143, (2008).
6. J. Laarni, L. Norros and L. Salo, "Multi-stage Approach to Control Room Validation", Presented in *OECD/NEA WGHOF Task Group*, (2015).
7. Z.C. Roza, J.M. Voogd and D. Sebalj, "The Generic Methodology for Verification and Validation (GM-VV) to Support Acceptance of Models, Simulations and Data", Amsterdam, National Aerospace Laboratory, (2014).
8. J. Laarni, P. Savioja, L. Norros, M. Liinasuo, H. Karvonen, M. Wahlström, and L. Salo, "Conducting stepwise HFE validations to support control room modernization", In Proceedings of *ISOFIC/ISSNP 2014*, Jeju, Korea, August 24-28, (2014).