Paper presented at the IAEA Second international Symposium on Nuclear Power Plant Life Management, Shanghai, China, 15-18 October 2007.

Research in automation, risk analysis, control rooms and organisational factors; applications to plant life management

B. Wahlström, J.J. Hämäläinen, J.-E. Holmberg, U. Pulkkinen, K. Simola, K. Juslin, L. Norros, H. Harju, T. Reiman, I. Karanta

VTT Technical Research Centre of Finland
P.O.Box 1000, FI-02044 VTT (Espoo), Finland

Abstract. Nuclear power is qualitatively different as compared with many other technologies. The differences are connected to factors such as very long time spans, the need for broad and deep knowledge, a large accident potential and political controversies. Before a country can enter a nuclear power programme it is important that these issues are understood and acted upon. The paper describes the nuclear power programme in Finland from the view of a technical support organisation with a special emphasis on automation, risk analysis, control rooms and organisational factors. It is argued that research and development are important components in maintaining nuclear knowledge in a country. Research at VTT within the four areas mentioned is described in more detail to illustrate some important issues that have to be resolved on a medium term to ensure a continuing success of nuclear power. A conclusion of the paper is that major stakeholders in nuclear power in a country have to co-operate on a neutral platform. Research can serve as an ideal platform for such co-operation.

1. Introduction

Nuclear power is qualitatively different as compared with many other technologies. The differences are connected to issues such as the need to bridge very long time spans, the need for broad and deep knowledge in several disciplines, the large accident potential of nuclear power plants (NPP) and political controversies that are connected to the nuclear technology. This implies that a country entering a nuclear power programme has to commit itself to support the necessary infrastructures over the life time their NPPs. Important for this infrastructure are the so called technical support organisations (TSO) that support both the regulatory authority and the nuclear utilities.

The paper describes the nuclear power programme in Finland from the view of the Technical Research Centre of Finland (VTT) which serves as a TSO for the nuclear field in Finland. VTT has a very broad competency in nuclear power in several fields such as reactor modelling, thermo-hydraulics, fuel calculations, environmental modelling, waste handling, risk analysis, materials, automation, human factors, management systems and organisational culture. The present paper puts special emphasis on automation, risk analysis, control rooms and organisational factors and gives more detailed descriptions of recent research results in these areas.

2. Commitment to nuclear power

A major challenge in nuclear power lies in the very long time that has to be bridged over the life of a NPP. From the first decision to start a NPP project, it may easily take five years to get the first approval to make it possible to ask for tenders. The preparation of a tender may take a year even for an experienced vendor and the evaluations and negotiations perhaps another year. The regulatory review for a construction license may also take a year. Thus even if the construction time for the plant could be squeezed to five or six years, the total time of getting the plant on line can easily slip to 15 years. If the planned operational life of the plant is sixty years, a century may easily have passed before the plant has served its operational life and has been decommissioned. In practice this means that at least three generations of people have to serve the plant and that it has to go through several large

technological changes during its life time. The need to plan for such long time periods demands a good understanding of the requirements nuclear technology sets on people and organisations during plant design, construction, operation and decommissioning.

The long life time of NPPs and the special characteristics of the technology imply that there should be a lasting societal commitment to nuclear power that can grant the operators of the plants industrial peace for doing their job in a serious and prudent manner. Nuclear power also puts a demand on national infrastructures, which should include a functioning legislative environment, a good educational system, support for research and development, and a businesslike regulatory regime. If a proper operational environment is available, the nuclear utilities can control other preconditions for their safety and economy, such as high ambitions, good international contacts, plant autonomy, enough staff, a motivational climate, safety culture etc.

3. Nuclear power in Finland

Finland has today four operating reactors, two PWRs at the Loviisa site and two BWRs at the Olkiluoto site. In addition a new PWR is under construction at the Olkiluoto site. The reactors at the Loviisa site were taken into operation in 1977 and 1980 and the reactors at the Olkiluoto site in 1978 and 1980. The new EPR type reactor is planned to be taken into operation in 2010. The reactors in operation have gone through extensive modernisations, which among other improvements also have resulted in power upgrades. The operational results for the four reactors have over the years been excellent.

3.1.The energy situation in Finland

Finland is a small country with about 5,3 million inhabitants. The electric grid is interconnected with the grids in Denmark, Norway and Sweden and it has DC connections to Estonia and Russia The consumption of electricity in the year 2006 was nearly 90 TWh, which was supplied from hydro 11,3 TWh (12,6 %), nuclear 22,0 TWh (24,4 %), CHP 27,6 TWh (30,6 %), condensation power 17,5 TWh (19,5 %), wind 0,2 TWh (0,2 %) and net imports 11,4 TWh (12,7 %). The annual electricity consumption has since 1980 been increasing annually with an average of 3,2 %. In Finland there is presently a strong political commitment to fulfil the conditions of the Kyoto protocol.

Nuclear power has since the end of the 1960's been on the agenda as an option for responding to increasing demands for electricity. In 1986 the plans for additional nuclear capacity had advanced to a point were an application to build a fifth reactor was about to be submitted to the government. That time the Chernobyl accident made the plans politically impossible. The next time the issue was brought to the political agenda was in 1993, when the Finnish parliament voted on a resolution on nuclear power. The pro-nuclear constellation lost the vote and the issue was shelved once more.

An increasing consumption of electricity and a larger dependence on imports together with the concern connected to CO_2 emissions and global warming brought nuclear power on the agenda a third time in 2002. This time the vote for the construction of a new nuclear reactor was positive. The investment decision and plant selection were made in 2003, the construction license application was filed early 2004, the excavation on the site started in the winter 2004 and the construction started in the spring 2005. The commercial operation of the Olkiluoto 3 plant is expected to start in 2010. This plant is only expected to decrease the gap between supply and demand in 2020 and therefore discussions on a sixth reactor have been initiated. TVO and Fortum have carried out environmental impact assessment of building a new reactor at the Olkiluoto and Loviisa sites. Moreover, international companies have indicated interest to build new reactors at other sites in Finland.

3.2.Nuclear research in Finland

In Finland the importance of investing in knowledge got a broad support from the very start of the nuclear power programme in the late 1960's. At that time research groups were established under the auspices of the Ministry of Trade and Industry to establish a knowledge base in reactor analysis,

thermo-hydraulics, materials science, instrumentation and control, and reliability engineering. The groups were transferred to VTT in the beginning of the 1970's. The research activities expanded over the years and they were instrumental in building the base for the first four reactor units. From the 1980's these activities were organised as national research programmes. In hindsight, it is very clear that the programmes have had a profound influence on the success of nuclear power in Finland.

The present structure of the national research programme was established during the programme, running in the period 1999-2002 [1]. The programmes are administrated by a steering group nominated by the Ministry of Trade and Industry (KTM). The steering groups typically consists of representatives from Radiation and Nuclear Safety Authority (STUK), Ministry of Trade and Industry (KTM), Technical Research Centre of Finland (VTT), Teollisuuden Voima Oy (TVO), Fortum Power and Heat Oy, Fortum Nuclear Services Oy (Fortum), Finnish Funding Agency for Technology and Innovation (Tekes), Helsinki University of Technology (TKK) and Lappeenranta University of Technology (LTY).

The key research areas in the programme during the period 2003-2006 were 1) reactor fuel and core, 2) reactor circuit and structural safety, 3) containment and process safety functions, 4) automation, control room and information technology, 5) organisations and safety management, and 6) risk-informed safety management [2]. The research programme included annually over 20 research projects, whose volume varied from a few person months to several person years. A complete description of the projects is available in the final report from the programme [3].

The present research programme [4], which is planned to run until 2010, is strongly based on the chapter 7a, “Ensuring expertise”, of the Finnish Nuclear Energy Act. This programme will address the following areas, 1) Organisation and human factors, 2) Automation and control room, 3) Fuel and reactor physics, 4) Thermal hydraulics, 5) Severe accidents, 6) Structural safety of reactor circuit, 7) Construction safety and 8) Probabilistic safety analysis (PSA). In 2007 there are altogether 30 research projects and volume of the programme is planned to be 46 person years and 6.3 M€.

4. Nuclear research at VTT

The Technical Research Centre of Finland (VTT) is a governmental organisation that is specialised in applied technical research. The total staff at VTT is about 2800 people of which about 200 are connected to research in nuclear power. A specific characteristic of VTT is that the different fields of research are not supposed to serve only the needs of nuclear power, but are instead serving a broad industrial base in Finland.

4.1.Early research in instrumentation and control and reliability engineering

Early research in instrumentation and control (I&C) and reliability engineering provided a basis that has expanded to be divided into the present areas of automation, risk analysis, control rooms and organisational factors. These areas have also demonstrated their importance for the safety of nuclear power in the accidents at Three Mile Island and Chernobyl. VTT knowledge in the four areas has found practical applications in the licensing of the new plant in Finland. Present research work in the above-mentioned areas related to the plant life management deals with issues such as:

- I&C and control rooms modernisations,
- Implementing and licensing digital I&C,
- Risk informed decision making and licensing,
- Verification and validation of control room changes,
- Assessment and development of maintenance practices,
- Management systems for conservative decision making,
- Safety culture in organisational changes and the generation change.

The knowledge created in the research projects has been utilised in many ways. Firstly and most importantly it has made it possible to support both the regulator and the utilities in important matters

connected to design and operation of the plants. Secondly the knowledge has been engaged in many in depth studies of various issues. Finally both the utilities and the regulator have been able to use the researchers as a resource pool for their own recruitments, which has made it possible to maintain a sound age profile at VTT. The researchers at VTT have been successful in networking both with other national research organisations and with international organisations.

4.2.Recent and on-going research projects

Several research projects at VTT within automation, risk analysis, control rooms and organisational factors are funded from the Finnish national research programme, but many projects are also commissioned by contracts with organisations and companies both in Finland and abroad. The division below does not follow the divisions into projects, but is instead a more general area oriented division.

4.2.1. Risk-informed safety management

Risk-informed safety management implies the use of information from probabilistic safety assessment (PSA) to support decision making in various contexts. In nuclear safety regulation, risk-informed applications supplement deterministic licensing practices. The Finnish regulatory PSA guide calls for risk-informed assessment of safety classification, in-service inspection programmes, in-service test intervals and allowed outage times of equipment. Similarly, maintenance and surveillance programs, training of personnel, working out of procedures and ways of acting can be assessed.

The research at VTT has dealt with both developments of risk-informed methods and specific PSA modelling issues related to uncertainties that can hinder implementation of risk-informed applications [5]. The main objective has been to develop risk-informed decision making methods integrating results from risk and reliability analyses with other expertise in the domain, to develop assessment methods for plants' operation and maintenance, to enhance planning of activities and acting in situations and to develop PSA methodologies. The results of the research activities have direct applications in risk-informed decision making both at nuclear safety authorities and utilities.

The focus of human reliability analysis has traditionally been on human performance in disturbance conditions. Of equal importance are however human errors in planning, design and maintenance, because they may introduce latent deficiencies in the system. Possible common cause failures (CCF) that have a human origin may affect the core damage probability significantly. This topic has been addressed in studies, where occurrences of latent human errors have been searched for and analysed in detail from the maintenance history in the Finnish NPPs [6]. A process model for planning a risk informed and cost-effective maintenance programme has been constructed [7]. The model covers risk management objectives and criteria such as risk importance, avoidance of production losses and CCFs. The approach supports the utilities' planning, updating and analysis of the maintenance programme.

Method development for risk-informed in-service inspection (RI-ISI) has been carried out to support the implementation of RI-ISI in the Finnish regulatory environment [8]. The applicability of a rough quantitative categorisation of the piping failure probability combined with conditional core damage probabilities obtained with a plant specific PSA was examined. The study included development of a probabilistic fracture mechanics (PFM) analysis procedure, and an approach to combine PFM and Markov system analyses to investigate inspection strategies.

A method has been developed for supporting risk-informed management of fire situations at the plants [9]. One purpose of the method is to enable the sharing and integration of relevant expertise from different domains. The method provides a frame of reference that facilitates crossing of disciplinary boundaries and it can be used to gain a better understanding of the controllability of fire situations. A scenario analysis method has been created for the analysis of different fire situations. It includes the identification of critical assessment tasks and analysis of possibilities for the involved actors to make better assessments in fire situations. A network analysis method has been developed for considering the controllability of fire situations from the co-operational point of view. The method can be used in

the development of control room procedures operator training and the fire alarm system. It also supports the development of co-operation between control room operators, fire fighters and other relevant parties to improve the realism of fire PSA.

Computer based systems have an increasing influence on the operation of NPPs. With programmable technology it is fairly straightforward to implement the required functionality for controlling different processes of a NPP. On the other hand the programmable technology may introduce unwanted complexity and new failure modes to the I&C systems. A reliability estimation methodology based on Bayesian inference has been developed and more recently the methodology has also been applied from a PSA point of view [10].

The software reliability of a motor protection relay was assessed in a case study. Expert judgements of the different developer groups of the relay were applied as the prior estimate of the relay failure probability. The prior estimate was built into an expert judgement process, where the technical documentation of the relay was reviewed and uncertainties within and between the development groups were recognized and estimated. The prior reliability estimate given by the experts was updated to a posterior estimate with available reliability data from relay testing and operational experience. The reliability estimation method for computer based systems provides justified failure probabilities to be used in quantitative reliability analysis of safety functions that are implemented using programmable technology.

4.2.2. Simulators for analysis, training and testing

Simulators have an important position both in modernisation projects and new builds. They can be used for developing and testing control algorithms, for the preparation of safety cases and for the verification and validation of control room functions. The development of the multifunctional APROS simulation tool was commenced in 1986 as a joint effort between Fortum and VTT [11]. APROS is now a commercial product that has users in 21 countries. It is for instance used at the HAMMLAB facility in Halden, Norway for research in human system interfaces (HSI). In the development of the APROS platform several important requirements were considered as elaborated below.

A simulation platform should perform as carrier of plant information from designers to different generations of users, for the whole life cycle of the plant. The APROS Specification Language is a script for specification of both process and automation component parameters and their connections. It can be stored as an ASCII file for transportation of the model specifications between evolving computer and operation system platforms. The specification of a plant model requires accordingly neither writing of equations nor programming.

A simulation platform should be reliable enough for testing of new designs and transients. The APROS simulation engine is extensively verified and validated before the release of new versions. The general philosophy is that the functionality of each building block is verified in a sufficient number of configurations and conditions based on measured transient from test facilities. APROS also includes the functionality of electrical and control systems.

A simulation platform should run in real time on affordable computers configured with full scope power plant models. APROS has efficient solvers for homogeneous and separated phase thermal hydraulics as well as for one and three-dimensional neutronics. APROS has also solvers for plant electrical systems as well as for automation systems. The fast access steam tables reach well beyond the critical pressure. Other substances than water and steam can be included in the flows. APROS Communication Library, an OPC interface and DLL interfaces enables communication with other programmes and codes.

During the years, APROS has been used for plant analysis, advance testing and control system improvements of the Loviisa plant. The models have grown from standard nuclear plant analysers to include containment and auxiliary system models that are needed in a full-scope training simulators. The renewed safety analyses studies that were needed to license the uprated 1500 MW_{th} power level of

Loviisa plant was generated with APROS. The platform has proved to be an excellent tool for safety analysis and Fortum Nuclear Services is currently doing practically all safety analyses with it.

APROS is presently used as a development simulator for the new man-machine interface in the I&C renewal of the Loviisa plant [12]. Currently the development system includes both operating and monitoring facilities of the new I&C systems Teleperm XP and XS. It has been used for functional validation of the HSI. The renewal at the two Loviisa units will take place during four consequent refuelling outages. APROS has been shipped to the suppliers' site in Germany for factory tests of the new systems and their configurations before the shipments for installation at the site. During first outage only limited automation functions will be replaced, during the second the safety critical automation will be in turn, during the third the primary system automation and during the fourth the secondary system automation. The training simulator HSI needs to be upgraded accordingly. Loviisa 2 is following the schedule of Loviisa 1 with a delay of two years. Different training simulators are thus needed for the separate plants having different control room layouts. The development simulator is therefore used to support the present training simulator of the Loviisa plant.

4.2.3. Development of control rooms

The development of control rooms is an important task both for the four older reactor units in Finland and for the new unit being built. The research has focused on an integrated validation of complex HSIs, which is anticipating the needs for knowledge, methods and know-how concerning human factors evaluations that the modernisation of the Finnish NPPs and their control rooms will bring. The evaluation needs become even more pressing in the construction of a new nuclear installation with digital I&C and a screen-based control room. This implies that the new control room functions have to be validated before they are implemented. The validation of human-system interfaces is a widely identified challenge and appropriate methods should be used for this task [13]. The following design rationale defines the theoretical basis of the method called Contextual Assessment of Systems Usability (CASU):

- "Systems usability" as an integrative evaluation basis.
- The evaluation should support both design and regulatory acceptance of new designs.
- An adequate definition of the underlying evaluation basis for good design.
- Understanding the connection between interface features and operator performance.

Systems usability of a complex HSI implies that the technology should be evaluated in a holistic and context dependent way. The technology must therefore facilitate the core task of particular tasks. Furthermore the technology must fulfil three generic functions of tools, i.e. the instrumental, psychological and communicative. Systems usability therefore means that that the tools induce desired effects, they fit and shape the human dispositions to act correctly and they communicate the relevant context to the users in a meaningful way. The evaluative dimensions of efficiency and effectiveness, fitness for human use and meaningfulness are therefore used. Systems usability is visible in the users' work performance as systems usability promotes the construction and development of work practices.

The essence of CASU method is depicted in Figure 1. The inference process consists of four separate phases. The coloured boxes denote research activities and the white boxes are the outcomes of the activity. The first phase, the modelling phase, outlines the basis for the evaluation by producing a reference. Here it is stated what good process control activities in given operational situations are. The modelling phase includes a task analysis, because task demands defined both in functional and sequential form is the output of the model. This is the first approximation of the core task. The important outputs of the modelling phase are the core task oriented measures and criteria used in the control room evaluation.

The second phase is the data collection phase in which the actual simulator runs or other performance situations are observed, videoed and covered in interviews. In the CASU methodology the data collection methods vary between activity observations, questionnaires and a few types of interviews. Data collection can be carried out either in a simulator or in a normal work situation.

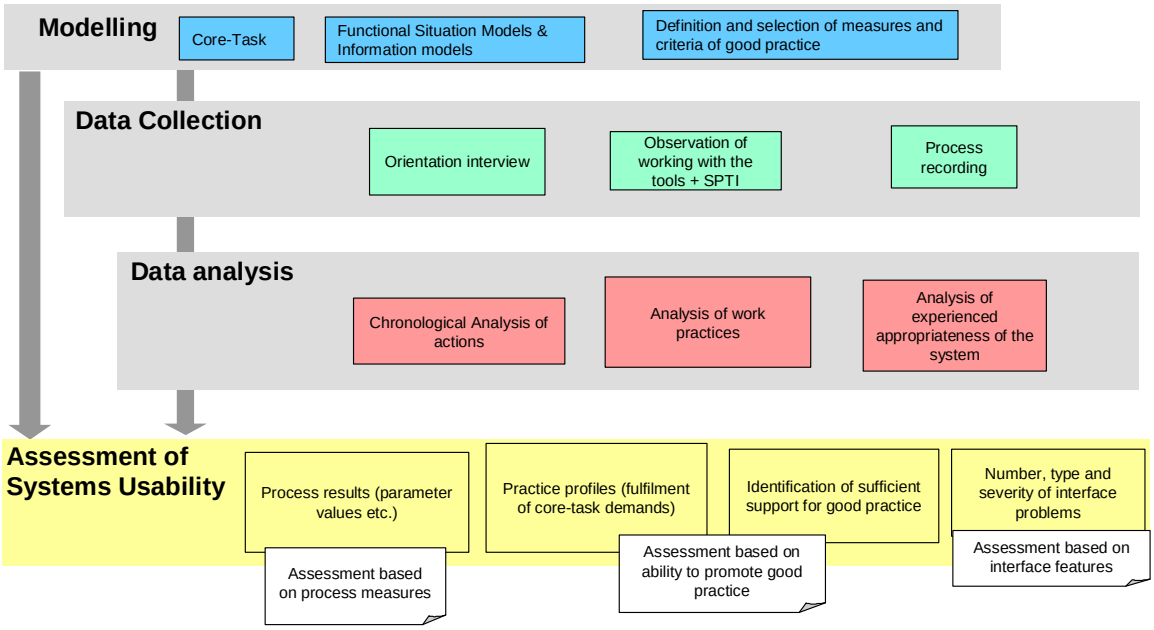

FIG. 1. The principle inference structure of evaluations proposed in the CASU method. (Abbreviation SPTI refers to situational process-tracing interviews).

The third phase is the analysis phase. Analysis aims at taking different perspectives to the collected data. First the observation data is analysed from chronological point of view, i.e. what happened in the scenario and when. This information is combined to create a performance analysis. From trends and logs it is possible to see how the process behaved and whether main parameters remained within acceptable boundaries. In the analysis part, the crew's practices of process control are assessed. This is done based both on observable behaviour and on the justifications the crew gives for their own actions. In interaction analysis, the HSIs are observed and analysed on a detailed level. The experienced appropriateness is analysed based on the interview data. The evaluation ends with the assessment of the interface. The assessment is thus made by combining three points of view: Process measures, the tools ability to promote appropriate work practices and interface quality.

On the basis of evidence collected so far, the method has proven its capability as an integrated validation method. The synthesis of evidence for acceptance arises from repeated and diverse reviewing, testing and discussing. Proof for safety and usability could be offered in the form of a combined safety and usability case. This type of reasoning can provide a method to accumulate evidence for acceptability from the design process of the HSI.

4.2.4. Smart devices with embedded software

Smart devices with embedded software are used at an increasing rate in modern I&C. The licensing of these devices implies an assessment of so called COTS (commercial-off-the-shelf) solutions, which can be very difficult if the device has to be treated as a black box. The assurance of smart devices for use in critical applications requires the safety assessment of their software. The goal of the research [14] was to develop a generic safety case approach for such software that takes into consideration: 1) the particular issues of assessing COTS software and the design and accessibility of smart devices; 2) regulatory requirements in Finland and 3) current practices of software assurance developed in Finland, UK and European projects. The project was carried out in co-operation between VTT and the British company Adelard LLP.

A safety case is defined as "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" [15]. Evidence can be deterministic (e.g. mathematical proofs, logical reasoning etc.), probabilistic (e.g. Markov model, fault tree) or qualitative (expert judgment). The purpose of a safety case is to make

such an argument clear, comprehensive and defensible [16]. The main elements of a safety case are [17]:

- *Claim* about a property of the system or some subsystem.
- *Evidence* which is used as the basis of the safety argument. This can be either facts (e.g. based on established scientific principles and prior research), assumptions, or sub-claims, derived from sub-argument on a lower level.
- *Argument* linking the evidence to the claim, which can be deterministic, probabilistic or qualitative.
- *Inference*, the mechanism that provides the transformational rules for the argument.

Figure 2 shows a schematic representation of a safety case. The generic structure is based on the following principles:

- *The safety cases are layered*, i.e. there exists a top-level safety case which has subsidiary safety cases for each subsystem.
- *There is traceability between system and subsystem levels*, i.e. top-level requirements are transformed to derived requirements such as security and maintainability; these in turn, are converted into design requirements that are implemented in one or more subsystems. The subsidiary safety cases for the subsystems identify design features and present arguments to support claims that they implement the safety attributes.
- *Design for assessment*, i.e. the production of the safety case is integrated with the design of the system. Some candidate design options are identified and a preliminary safety case is constructed. The latter consists of iteratively identifying hazardous subsystem states (e.g. through hazard analysis) and appropriate countermeasures (elimination, reduction, failure mitigation). The design and the safety case are then assessed to establish whether 1) the design implements the safety functions and attributes, 2) the design criteria are satisfied, 3) the design is feasible, 4) the associated safety case arguments are credible and 5) the approach is cost-effective.

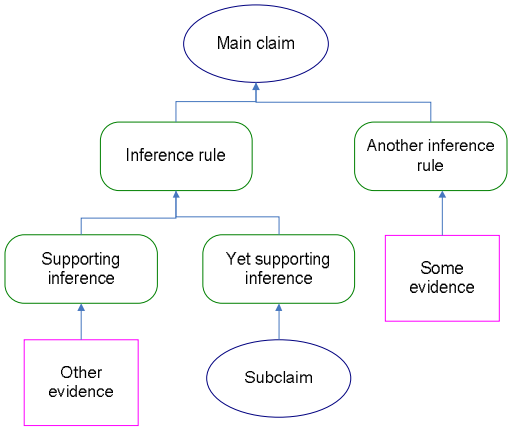

FIG. 2. A schematic representation of a safety case.

The approach was based on safety cases, requirements specifications for the automation systems, the theory of argumentation, and on applying systematic procedures throughout. The specific issue addressed in detail was the assessment of COTS. In COTS, there is often missing or insufficient evidence, e.g., no source code is available. The feasibility of the approach was demonstrated through a study of the safety case for a smart device, Site Programmable Alarm unit. The unit provides a monitoring function for signals from temperature and other sensors and monitoring equipment. Alarm outputs are triggered when high or low limit values are exceeded or on the rate of change in input; the trigger parameters are fully programmable. The approach developed is a goal based method in which claims are defined, elaborated and apportioned after which the required arguments are identified to illustrate the claims. An expert has to assess whether the claims are satisfied in the light of available evidence.

4.2.5. Software qualification

Software qualification is an essential part in ensuring functionality of digital I&C. Research has been carried out with a classification of error types and methods for error management in software life cycles. The objective of the research was to create recommendations for the inspection of documents and other application artefacts of software-intensive I&C systems [18]. The recommendations that are based on existing standards and regulations (e.g. YVL 5.5, IEC 60880, IEC 62138) aim to

- Determine error types of application software documents,
- Clarify effectiveness of error management methods for determined error types.

A new approach for classifying software errors based on linguistic concepts has been developed. Errors were divided into three classes

- *Syntactic*: an inconsistency between the item presented in a document and the language in which the document was written
- *Semantic*: an inconsistency between the document and information in another document or domain
- *Pragmatic*: an inconsistency between the document and the users' or computers' interpretation of it, or a failure to use the document.

The proposed computer semiotic classification was validated by a number of incidents involving software errors. To make error management comprehensive, the management process should use diverse methods. In order to evaluate the comprehensiveness of the process, each management method should be evaluated against every error type. The artefacts considered were requirements specifications, design documents, test plans, test results, and analyses. Error management was considered from the perspective of error types. Recommendations to users were given on selecting error management methods that supplement those of the I&C systems suppliers. Recommendations for evaluating application software documents were also given. Estimation of the likelihood of software error types in an I&C system was considered both from the users' and inspector's point of view. The error types and error management methods were combined into a hierarchical representation in order to evaluate the effectiveness of different methods for preventing and tolerating the three error types.

4.2.6. Management systems

Management systems can be seen as the software of an organisation. Basically they should provide a businesslike approach to management, which offers systematic, explicit and comprehensive processes for managing safety. The management systems include processes for goal setting, planning and assessing performance. A management system is woven into the fabric of an organisation and it becomes part of the organisational culture, i.e. the way people do their jobs. More practically the management system can be seen as a tool that

- documents practices and ways of working,
- serves as a reference in different situations, i.e. defines what is allowed and what is not allowed to give confidence to managers and co-workers,
- gives a norm for audits and reviews,
- is intended to engage and motivate the personnel,
- describes the organisation to outsiders.

Research related to management systems was carried out in the EU-projects called ORFA [19] and LearnSafe [20]. Building on that base VTT has together with the NPPs in Sweden entered a co-operation that aims a shedding light on requirements to be placed on management systems. Discussions so far have found a general agreement that the management system should

- exist and be documented,
- be understood, accepted and used,
- be reasonable complete,
- contain descriptions of organisational structure, positions, roles, responsibilities and authorities,

- contain descriptions of requirements and solutions to be documented in instructions, methods, tools and practices,
- take a graded approach towards safety,
- be assessed, audited and updated at regular intervals.

Experience has however shown that these requirements are not always fulfilled and management systems are even sometimes considered to be an additional burden in the work [21]. The research has addressed the application of available guidance on management systems as well as more generic elements such as organisational structures and decision making. Important issues to investigate are how the management systems can be adapted to people and how the division of responsibility between systems and individuals should be defined. Present studies will be followed up by a project, which takes a closer look on the processes that are used for safety reviews of various documents at the NPPs.

4.2.7. Organisational culture

Organisational culture is a key in determining how an organisation manages safety. The research has focused on three themes: organisational changes, high reliability organisations, and methods for assessing organisational culture. VTT has developed Contextual Assessment of Organisational Culture (CAOC) methodology (cf. Figure 3), which has been the main methodology in the research [22].

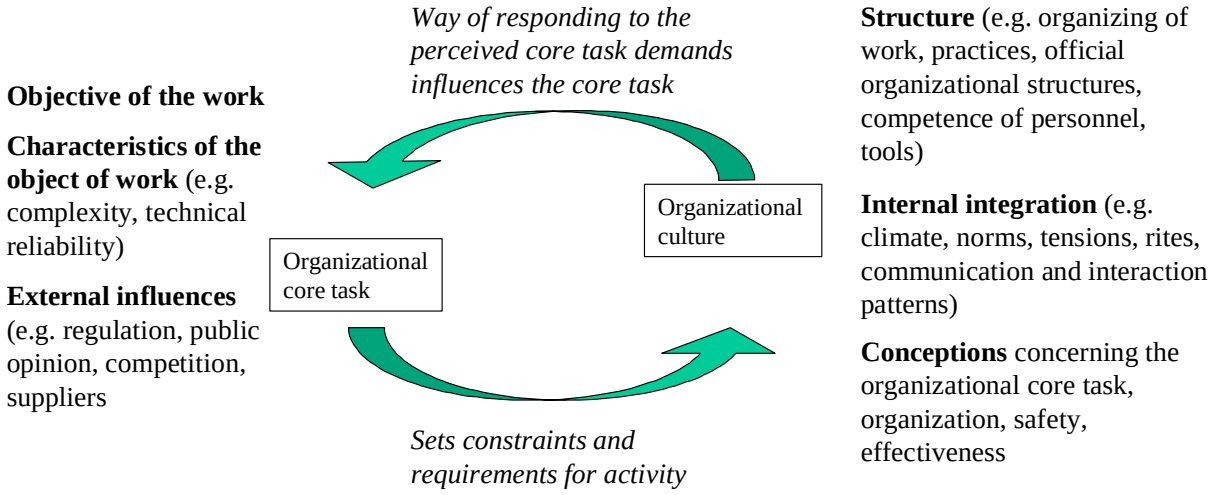

FIG. 3. The central concepts of CAOC and their interrelations.

The methodology utilises two concepts, organisational culture and core task. The core task can be defined as core demands and content of work that the organisation has to accomplish in order to be effective (productive, safe and healthy). The core task concept can thus be used in assessing central dimensions of the organisation's culture. Organisational culture influences the definition of the core task, which in turn sets demands for the formation of culture. The core task model constructed in the study acts as a point of comparison when key features of culture are examining. The methodology has been applied in studying regulatory work at STUK and maintenance work at Loviisa NPP. The aim of these case studies was to model the core task of the organisation and to characterise its organisational culture. The methodology can also contribute to the design and redesign of work in complex socio-technical systems [23].

In studying organisational culture and management of change, the safety implications of various organisational factors were inspected [24]. Case studies were carried out in maintenance and engineering departments at the NPPs in Finland and Sweden. The safety effects of organisational changes were modelled together with Swedish researchers [25]. The special characteristics of safety critical organisations from a work psychology perspective were also described [26].

The objective of present research is to study the facilitators and hindrances to organisational learning and to the development of safety culture in the nuclear power industry. The aim is to help power companies and the regulator to create safety management practices that support the evaluation and management of working practices and organisational performance. Issues that are addressed in the research are the utilisation of operating experience, organisational reviews and safety culture in subcontracting. Furthermore, methods and models for safety management and organisational learning are created for both the regulator and the utilities.

4.3. International co-operation

VTT has over the years built and maintained a large network of international co-operation. Important for the contacts have been the Nordic nuclear safety research, IAEA and OECD/NEA. When Finland joined EU in 1994 a new channel opened to European R&D and Finland and VTT has since then been actively involved-in several consortia with funding from EU through the EURATOM programme. Other important contact channels have included the TSOs in France, Germany, Japan, the UK and the USA. In the area of automation, risk analysis, control rooms and organisational factors the OECD Halden Reactor Project has been an important partner to VTT over many years. The contact networks have been important also in the recruiting and training of young engineers and scientists.

5. Conclusions

Plant life management has got increased attention over the last decade. Plant life management should, however, be seen in a larger context than just materials and ageing of major components. It is also important to see plant life management in the context of creating and managing a national infrastructure of competence that may be depleted if not nourished over time. TSOs have an important strategic mission in co-operating with the regulatory agencies and the nuclear utilities in this task.

Research and development are important components in maintaining the knowledge needed for design, construction, operation and decommissioning of NPPs. The research within automation, risk analysis, control rooms and organisational factors at VTT has shown to provide an efficient systems base for many of the considerations that are important in a plant life management perspective. These four areas have also over the years proved to be able to respond to new demands that have emerged both in the analysis of present designs and in the synthesis of new solutions for an improved safety. The research that presently is undertaken at VTT is well adapted to the needs, which are seen on a medium term in ensuring a continuing safety and economy of the NPPs in Finland.

The publicly funded nuclear safety research has demonstrated the benefit of a neutral platform for co-operation among major stakeholders in Finland. There are two keys to the success. The first one is that the research has concentrated on mid-field issues, i.e. issues of a technical and scientific content that are of interest both for the nuclear regulator and for the nuclear utilities. The second is that public funding has to be available to make it possible to concentrate on issues that are relevant in a medium or long term [27]. Such mid-field research has provided an ideal platform for co-operation between the Finnish stakeholders in nuclear power.

REFERENCES

[1] Kyrki-Rajamäki, R., E.-K. Puska, (eds.): FINNUS. The Finnish Research Programme on Nuclear Power Plant Safety, 1999-2002. Final Report. VTT Research Notes 2164 (2002).
[2] Puska, E.-K. (ed.): SAFIR. The Finnish Research Programme on Nuclear Power Plant Safety 2003-2006; Executive Summary, VTT Research Notes 2364 (2006).
[3] Räty, H., E.-K. Puska, (eds.): SAFIR. The Finnish Research Programme on Nuclear Power Plant Safety 2003–2006, Final Report, VTT Research Notes 2363 (2006).
[4] http://virtual.vtt.fi/safir2010/.
[5] Holmberg, J.-E.: Principles and practices of risk-informed safety management, PPRISMA summary report. In [3].

[6] Laakso, K.: Systematic analysis and prevention of human originated common cause failures in relation to maintenance activities at Finnish nuclear power plants, STUK-YTO-TR 217, STUK, Helsinki (2006).
[7] Laakso, K., P. Luukkanen: Development of maintenance strategies for a nuclear power plant. 18th Euromaintenance 2006 and 3rd World Congress of Maintenance, June 2006, Basel.
[8] Cronvall, O., I. Männistö, K. Simola: Development and testing of VTT approach to risk-informed in-service inspection methodology. VTT Research Notes 2382 (2007).
[9] Hukki, K., J.-E. Holmberg: Development of Management of Nuclear Power Plant Fire Situations. PSAM 7 – ESREL '04, Berlin, Germany, June 14–18, 2004.
[10] Helminen, A., U. Pulkkinen: Quantitative reliability estimation of a computer-based motor protection relay using Bayesian networks. SAFECOMP 2003 – Computer Safety, Reliability and Security, Edinburgh, United Kingdom, Sept. 23-26, 2003.
[11] APROS 5.05 - Overview, http://virtual.vtt.fi/apros/overview.htm (2005).
[12] Ahonen, A: Simulators in I&C Renewal of Loviisa NPP, International Youth Nuclear Congress, 18-23 June 2006.
[13] O'Hara, J., J. Higgins, J. Persensky, P. Lewis, J. Bongarra: Human factors engineering program review model, US Nuclear Regulatory Commission, Washington, DC (2002).
[14] Pulkkinen, U., R. Bloomfield: Assessment of smart device software, in [3].
[15] Bishop, P.G., R.E. Bloomfield: The SHIP safety case approach. Proc. SafeComp95 (G. Rabe, ed.), Belgirate, Italy, 11-13 October 1995.
[16] Wilson, S.P, T.P. Kelly, J.A. McDermid: Safety case development: current practice, future prospects. Presented at Safety and Reliability of Software Based Systems - Twelfth Annual CSR Workshop, Bruges, Belgium, 1997.
[17] Bishop, P.G., R.E. Bloomfield: A Methodology for Safety Case Development. Safety-critical Systems Symposium, Birmingham, UK, February 1998.
[18] Harju, H., J. Ranta, M. Välisuo: Software qualification – error types and error management in software life-cycles, in [3].
[19] Baumont G. et al: Organisational Factors; their definition and influence on nuclear safety, VTT Research Notes 2067 (2000).
[20] Wahlström B. et al: LearnSafe – Learning organisations for nuclear safety, VTT Research Notes 2287 (2005).
[21] Wahlström B.: Quality systems: Support or hindrance for learning, in Andriessen, Fahlbruch (eds.). How to Manage Experience Sharing: From Organisational Surprises to Organisational Knowledge, Elsevier (2004).
[22] Reiman, T., P. Oedewald: Contextual Assessment of Organisational Culture – Methodological development in two case studies. In [1].
[23] Reiman, T.: Assessing organisational culture in complex sociotechnical systems – Methodological evidence from studies in nuclear power plant maintenance organisations. VTT Publications 627 (2007).
[24] Reiman, T., P.Oedewald: Culma summary report. In [3].
[25] Reiman, T., P. Oedewald, C. Rollenhagen, U. Kahlbom: Management of change in the nuclear industry. Evidence from maintenance reorganisations. MainCulture Final Report. NKS-119. Nordic nuclear safety research, Roskilde (2006).
[26] Oedewald, P., T. Reiman: Special characteristics of safety critical organisations. Work psychological perspective. VTT Publications 633 (2007).
[27] Wahlström B., Carl Rollenhagen: Organisational factors and nuclear safety – issues to address in research and development, Joint 8th Annual IEEE Conference on Human Factors and Power Plants and 13th Annual Workshop on Human Performance/ Root Cause/ Trending/ Operating Experience/ Self Assessment, Monterey, CA, August 26-31, 2007.