Advanced Licensing and Safety Engineering Method - ADLAS®

Pekka Nuutinen, Satu Sipola, Antti Rantakaulio
Fortum Power and Heat Oy
Keilaniementie 1, 00048 Espoo, Finland,
Pekka.Nuutinen@Fortum.com, Satu.Sipola@Fortum.com, Antti.Rantakaulio@Fortum.com

ABSTRACT

Complex nuclear projects, with long supply chains require detailed understanding and management to succeed. One of the most important success factors is licensing, which has been very challenging in past years in many nuclear projects (both new build projects and modernization projects). To better understand the licensing aspects and the safety features that are behind the licensing requirements, the high level safety engineering method has been developed in Fortum (Finland). This new approach starts from the high level safety functions and takes these functions into the next level building up a map of safety functions indicating also their safety importance for the overall safety of the nuclear power plant design. This method has patent pending in Europe and is currently used in different nuclear projects.

1 INTRODUCTION

Licensing has been part of operations in Fortum, Finland, from the beginning of Loviisa VVER power plants' life cycle. 2 VVER units in Loviisa have been designed and constructed in 1970-1976 and commissioned in 1977-1979. From these days, the units have been developed, partly redesigned and operating licenses have been renewed. In Finland the operating license is valid 10 or 20 years at a time and every 10 years the periodic safety review is done.

Loviisa NPP automation renewal begun in late 1990's, when also the regulatory environment in Finland and Europe started a fast development. New NPP projects were started in Europe and both the industry and regulators started to prepare for fast growing nuclear field. Since this development has been partly learning from the experiences, some challenges are now seen in the complex regulatory environment. In Finnish case, the regulatory requirements are developing into the more descriptive way, in contrary as in the US NRC requirements. The challenge in this development is seen, since different requirements and their real impact and importance to the nuclear safety is not equal (categorization is not seen in the regulations). To tackle this challenge and to make licensing more comprehensive and better understood, the new approach is needed.

The tricker to start this new approach development was the automation renewal need in Loviisa NPPs. Aim was to replicate the functionality of existing automation system with new automation platform. During the project it became evident that also safety function functionality needed to be partly re-designed due to new, restricted regulatory requirements and a lot of licensing work has to be done by the owner, not only in the automation but also in the plant and architectural level.

The new ADLAS® approach starts from unique combination of the plant level functional and non-functional requirements and elaborating them to functional entities. The architecture is in the center of overall safety and the system level safety functions are included in the approach.

This new ADLAS® approach has been used in Loviisa automation renewal projects, as well as some other safety improvements, and the approach has been successfully used for licensing in many projects with Finnish Radiation and Nuclear Safety Authority.

2 LOVIISA VVER ACTIVITIES AS BASIS OF ADLAS®

Fortum is an operator and licensee for Loviisa NPPs, but at the same time Fortum is an engineering office. Basically all nuclear safety related design changes are planned and executed by Fortum. Some examples of design changes over the years are the following:

- Power uprate 9%
- Severe Accident Management (SAM) systems
- Bunkered pumping station
- Diverse Residual Heat Removal (RHR)

Large modifications are also ongoing in Loviisa NPP that are licensed by Fortum. Examples of ongoing projects where ADLAS® is applied are:

- Automation renewal
- Diverse fuel pool cooling

ADLAS® will also be utilised in the Hanhikivi-1 project which is the sixth nuclear power plant unit in Finland:

- Reactor plant licensing

ADLAS® method is also suitable for other nuclear or non-nuclear related safety critical applications where are requirements for engineering process and design solutions.

3 TRADITIONAL APPROACH OFTEN LACKS HIGH LEVEL ARCHITECTURE

Traditionally engineering requirements have been addressed to the general plant design – so called design basis. This way the safety aspects are taken into account, if the plant is not very different from the ones licensed already. Also in design modifications, the challenge occurs if the designed safety functions are changed when systems are modified.

The design basis is in many cases assigned to the systems or functions, however the higher level architecture (system of systems) is not included. In I&C area the architecture level has been under discussion widely in past years, when new power plants have been licensed and I&C modifications are current in many NPPs. However this kind of systems engineering approach has not moved to the other parts of the NPP. Figure 1 presents the traditional engineering approach used in nuclear industry.

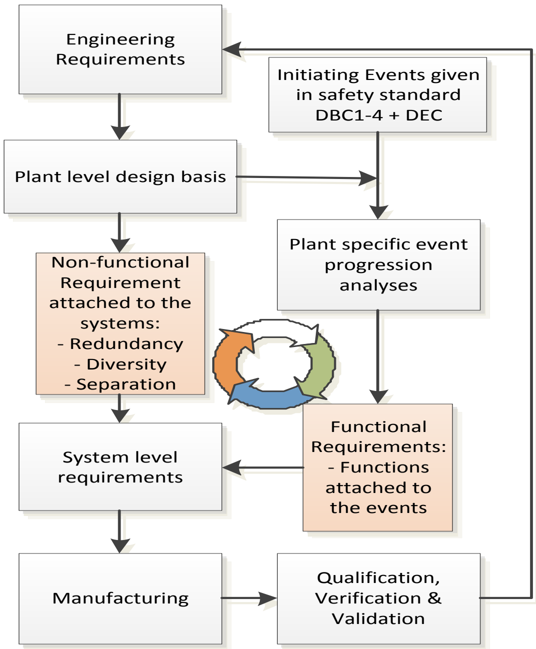

Figure 1: Example of traditional approach of engineering process

4 THE ADLAS® FOCUSING ON ARCHITECTURAL LEVEL COMBINES DIFFERENT LEVEL REQUIREMENTS

With Loviisa NPP modernization and safety upgrade projects, it has been noticed that the regulatory requirements are not directly applicable for plant design. High level conceptual requirements have been developed for the plant's safety.

Regulatory requirements need to be elaborated into the engineering requirements in every level. This work is not the core knowledge of the plant vendor, especially concerning:

- Safety critical digital automation
- Diversity concept
- DiD concept
- Verification and validation process in plant and architecture level
- Qualification
- Requirement management
- Configuration management

The new ADLAS® approach aims at solving these challenges effectively and efficiently. Requirements are first addressed to task categories, which are representation of defence-in-depth levels. Task categories are assigned to each event category taking into account the events timely behaviour and the required reliability target, which is realised by using redundancy, diversity and isolation/separation principles as well as quality requirements that are in line with the real safety relevance of the task category. Safety functions are assigned to task categories through which they receive non-functional requirements mentioned above. Technical architectures define systems which perform safety functions. This enables hierarchical and systematic requirement elaboration from the plant level to the system level. Figure 2 presents the new approach for engineering process.

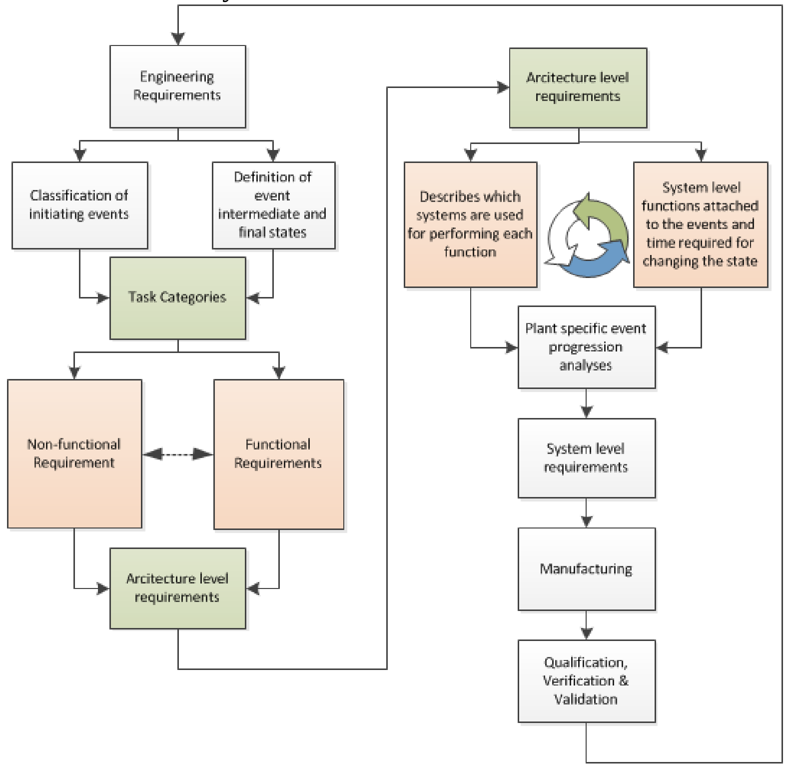

Figure 2: Example of new approach of engineering process

5 ADVANTAGES OF ADLAS THROUGH CASE EXAMPLE

ADLAS® provides a hierarchy to different level requirements. Figure 3 presents the basic idea of the different hierarchical levels for requirements.

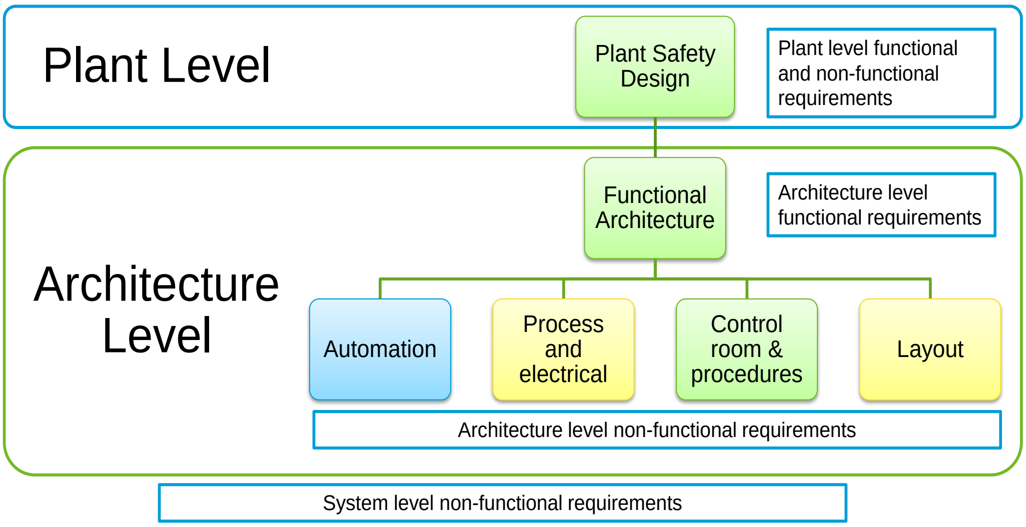

Figure 3: Hierarchical design of ADLAS ®

1. The main levels of the new approach and examples of the requirements in these levels are presented here: Plant level functional requirements - example: *bring plant to the controlled state after DBC3 with task category XXX*
2. Plant level non-functional requirements - example: *apply N+2 failure criteria for task category XXX*
3. Architecture level functional requirements - example: *In case of SBLOCA, inject coolant to the core with function YY00 in task category XXX*
4. Architecture level non-functional requirements - example: *For task category XXX, apply digital technology in automation architecture*
5. System level non-functional requirements - example: *For system ZZZ, implementing task category XXX, apply 4 * 100% redundancy*

The V-model (figure 4) as widely used for automation is now used also for other technical disciplines and upper level requirements, starting from plant level and going downward from there. This brings transparency into the overall engineering and licensing processes. In addition to automation discipline, V-model is used also for process, electrical, layout, control room and procedures engineering.

This transparent approach can take forward both safety level and understanding. It also helps coping licensing risks, providing the regulators better understanding of the big picture and therefore easing the approval process.

V&V plans and efforts are following design hierarchy. Aim of the verification ensures that products of design lifecycle meets requirements and aim of the validation ensures that products of the design life cycle are suitable for end use.

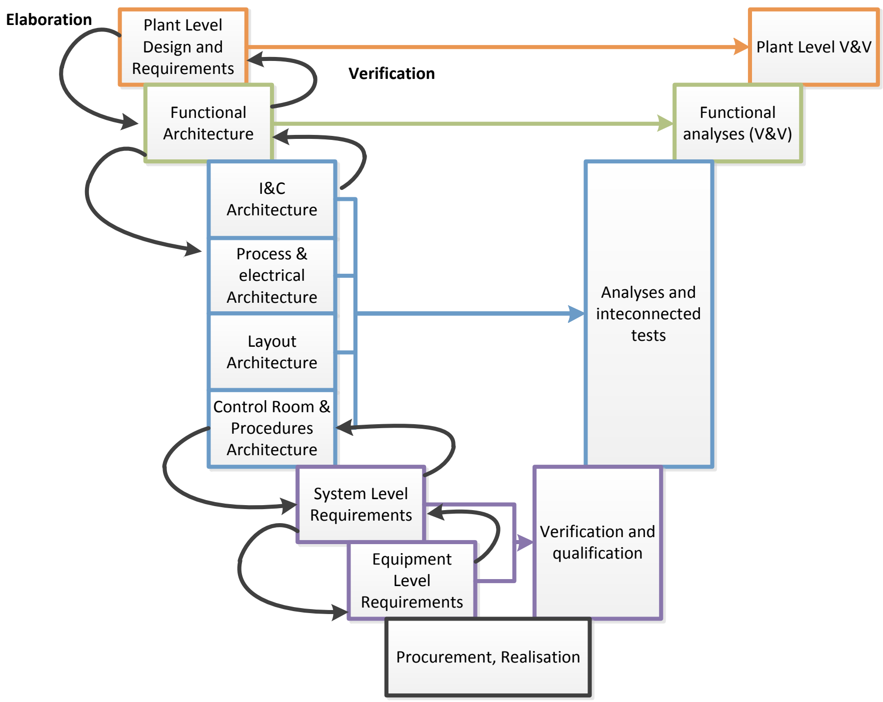

Figure 4: V-model as the basis of the approach

6 CONCLUSIONS

The new approach is introduced and it offers unique combination of the plant level functional and non-functional requirements and elaborating them to task categories. This enables hierarchical and systematic requirement elaboration from the plant level to the system level. V&V plans and efforts follow the design hierarchy and are used to ensure that products of design lifecycle meet requirements and validation to ensure that products of design lifecycle are suitable for end use.

The V-model is used to define design and V&V activities. All technical disciplines are covered. Use of the V-model brings transparency into the overall engineering and licensing processes. This transparent approach can take forward both safety level and understanding. It also helps coping licensing risks, providing the regulators better view on the big picture and therefore easing the approval process.

REFERENCES

[1] "Safety Critical System" Patent application number FI20155069