
Proceeding from the Safety Philosophy to Safety Requirements – Experience Feedback of TÜV NORD Group from Non-domestic Licensing Processes

Wolfgang Krüger, Dr. Volker Nitzki, Dr. Oliver Rabe

TÜV NORD EnSys Hannover, Am TÜV 1, D-30519 Hannover

Abstract:

It is a frequent experience from state-of-the-art licensing processes for nuclear facilities that a consistent approach to safety by implementing a Safety Concept is frequently missing in the respective planning of design, construction, commissioning and operation etc. The Safety Concept is understood as the combination of the technical and safety requirements to be considered during the different stages of the plant life cycle and the processes required for ensuring that the technical and safety requirements will be implemented appropriately throughout these stages. In a number of cases, the lack of a Safety Concept has lead e.g. to serious and unacceptable design deficiencies as seen from the safety perspective and to unnecessary complications on the way forward to a licence to construct. In the presentation, a top-down approach to an exemplary Safety Concept is described; the term "exemplary" stands for the fact that different approaches to implementing a Safety Concept may be chosen. This implies that specifically the process part of the Safety Concept is strongly governed by the respective licensing environment which in turn explains why a definite and universal Safety Concept for the licensing approaches in the different countries will not be feasible.

1 GENERIC LICENSING SITUATION OF THE NEW BUILD PROJECTS

Other than in the past ten to fifteen years, the planning and subsequent construction and erection of nuclear power plants is now reconsidered on a worldwide scale. TÜV NORD Nuclear is involved in licensing and operation supervision activities in a number of countries, like for instance Argentina, Brazil, South Africa, Sweden, South Korea, Finland etc., either on behalf of the licensee or the regulator. Part of the TÜV NORD Nuclear activities in this field relate to new build projects, either relaunched after a long period of stagnation or suspension or based on entirely new concepts which have not been realised so far.

The situation is similar in countries outside the current involvement of TÜV NORD Nuclear; i.e. a large number of new build projects are either planned or progressing. The common features of the new – or in some cases revived – projects are that

- each country has its own licensing approach – which should be self-evident and does not require further discussion,
- in the majority of cases, the established codes and standards as well as the regulatory environment are strictly applicable only to the already existing nuclear power plants,
- in a few cases, entirely new and unique plant concepts commonly denoted as Generation IV reactors are envisaged; usually, they are not enveloped by the existing codes and standards framework,
- due to the long suspension of new build activities in the past decades, licensing of any of the aforementioned projects is not a day-to-day exercise.

All of the above should not be too surprising, given the long phase of stagnation in the nuclear field. Removing the undisputable gaps and inconsistencies in the regulatory frameworks as well as in the codes and standards before starting the planning activities would be one option to provide a full and consistent set of acceptance criteria in licensing of new build projects. However, implementing a full, updated set of acceptance criteria before starting the planning and design processes would mean a probably undesirable loss of time and not necessarily contribute to safety: Ideally, such updating of the codes and standards should be accompanied by feedback from the planning and design activities on the feasibility and sensibility of the modified codes and standards. This means that an iterative process starting off from preliminary acceptance criteria and allowing for continuous improvements under consideration of the experience gained so far would be most efficient.

One conclusion from the above is that licensing the contemporary new build projects is featuring more of a challenge than the “bygone” licensing processes of the currently operating nuclear power plants which started commercial operation in the eighties and nineties of last century. It should be noted that this statement includes all parties in the licensing process and not to only the regulator.

The situation gets even more complicated if we take into account that the number of countries making use of nuclear power generation will supposedly increase in the near future. From a legal perspective, these countries should implement their own binding set of acceptance criteria as well as the procedural requirements in their respective licensing environment beforehand; however, this will also take some time – more time than usually tolerated by those who are involved in the licensing process of a nuclear power plant. Alternatively, reference to or implementation of internationally accepted codes and standards, like IAEA, ASME etc., is possible and might also be helpful, but this does not remove all the problems – on the contrary, this might even contribute to more trouble because there might be inconsistencies between the different sets of codes and standards.

There is the risk that the aforesaid is misunderstood or misinterpreted. Therefore, we want to point out that the net effect of the situation encountered frequently in contemporary licensing is not less care or accuracy in the licensing process; the top-most regulatory requirements – usually the necessary precaution and protection against the harmful effects of constructing and operating a nuclear facility – need to be fulfilled anyhow. However, the way forward to a licence starting off from the planning stage via the design phase up to the submittal and review of a Safety Case might not be straightforward any more and might even become unnecessarily arduous under the given circumstances. Unfortunately, this view is confirmed by the experience which we made in various new build licensing processes.

The above generic outline of the licensing situation for the new build projects gives rise to considering suitable approaches removing at least part of the foreseeable and predictable obstacles on the way forward to a licence. The objective of this presentation is to give an outline how the preparatory steps in the licensing process can be organised such that the aforementioned deficiencies can be removed and the plant design can be based on solid ground, even without having implemented a full set of acceptance criteria beforehand, i.e. at the beginning of the planning stage.

Before we discuss the outline of a suitable approach in more detail, we want to provide a few examples for inconsistencies identified in specific licensing approaches.

2 EXAMPLES FOR INCONSISTENCIES IN THE APPROACH TO ENSURING SAFETY

In the following we are listing a few deficiencies which are typical for the licensing approaches in contemporary new build nuclear projects as mentioned above. These examples reflect the experience which TÜV NORD Nuclear gained in several licensing processes. In our feedback, we address inconsistencies of both the technical and procedural requirements.

- Examples for insufficiently stipulated technical requirements are the lack of
 - a binding definition of the single failure criterion to be applied in the design process and in the safety analyses,
 - design requirements concerning the redundant system trains of the safety system,
 - a concept to determine the safety significance of the structures, systems and components (SSC) and to consider it appropriately in the design and safety assessment processes,
 - a concept to categorize the safety significance of issues to be licensed other than the SSC, e.g. site features, activities in commissioning etc.,
 - rules for the consideration of repair activities in safety systems during operation,
 - the acceptance criteria to be applied in the design and safety assessment processes,
 - a binding rule if and to what extent the inherent safety features of the plant may be considered in the design and safety assessment processes.

It was common practice in the situations which we are referring to that the design and safety analysts defined their own individual acceptance criteria. This gave rise to pronounced design and safety inconsistencies.

- On the procedural side, our most significant findings are as follows:
 - In a number of cases, the focus of the licensee and the other involved parties was exclusively on the preparation of the Safety Case which has to be submitted for granting e.g. a licence to construct. Preparing the Safety Case is typically a pre-licence activity. In the referenced cases, no effort was taken to provide for the processes which should be in place after the licence will be granted, i.e. the timely planning and implementation of the post-licence processes, like detail design, manufacture, construction and erection as well as commissioning in line with the respective licence, was neglected. This deviates from the usual approach which is to firstly base the licence to construct on basic (and not on detail) design and secondly finalise detail design at the latest possible stage in the design process, i.e. after the licence to construct has been granted. From a legal perspective, this requires to precisely define in the licence the processes and requirements to be adhered to in detail design.
 - Any nuclear project has a history. If the procedural requirements on reviewing and confirming design modifications, the achievement of licensing conditions etc. are fixed only insufficiently, a lot of information provided previously in the licensing process will be lost. This will inevitably lead to a not acceptable uncertainty about the licensing basis for a specific licensing step. If, for instance, a licence to construct is based on basic design information and the detail design of the plant is modified during construction without documenting and analysing these modifications properly, the concluding (and necessary) step of the construction stage – the statement that the plant has been constructed as "promised" in the application – will not be possible. From the regulatory

perspective, this means that the next step in the licensing process which usually would be commissioning will lack a basis.

In our understanding, the findings listed above make credible that a straightforward concept for implementing safety in the plant design is actually not self-evident and in a few cases even missing. This gave and gives rise to numerous deficiencies and inconsistencies which can only be overcome by implementing suitable approaches and processes. We are convinced that different alternatives for overcoming the aforementioned shortfalls are possible. In the following, we are proposing one such possible approach. The main feature of our proposal is the implementation and rigorous exploitation of the "Safety Concept". It is based on the TÜV NORD Nuclear experience gained in numerous licensing and operation supervision activities abroad (and in the domestic area).

3 THE SAFETY CONCEPT

3.1 Basic Remarks

What is the "Safety Concept"? We are offering a definition of this term below. Before we do so, we want to make a precautionary remark: It might be tempting to make statements like: "There is nothing new about this Safety Concept. We had it before; so, what is the benefit of the exercise?" We agree; however, experience tells us that awareness for the traditional approach is very often missing. This is why we address the topic as an issue of "Experience Feedback".

When we talk about the "Safety Concept", we have to distinguish it from the term "Safety Philosophy". We are not aware of any "official" definitions of these two terms. There might even be the understanding that distinguishing between these two terms should be marginal. Nevertheless, it is common practice to denote the safety features of the plant and their role in managing and accommodating the consequences of initiating events as the "Safety Philosophy", whereas the "Safety Concept" would describe the implementation of the Safety Philosophy. In other words: The Safety Philosophy deals with the "What" in nuclear safety, whereas the Safety Concept is focused on the "How".

Such distinction might appear to be arbitrary. However, the impact of these two features is different in the design and construction processes: As long as the Safety Philosophy remains unchanged, it provides input to the design process only at the start of the life cycle of the plant, whereas the Safety Concept governs the design, construction, commissioning etc. processes and would be extended permanently during the life cycle of the plant, for instance for the transitions from the construction and erection stage to the commissioning stage and further on to the operation stage. The Safety Philosophy means input only once, whereas the Safety Concept is a "living" feature which needs to be updated and enlarged permanently in line with progress in the life cycle of the plant. This implies that, for each of the life cycle stages, it provides for requirements and processes which need to be followed in the respective stages.

3.2 The Features of a Safety Concept

Before we carry on with a more detailed description of the Safety Concept, we want to make a few statements for the sake of clarification:

- The Safety Concept as outlined in this presentation reflects our understanding and use of this term. We do not exclude that other definitions or another terminology exist for the same issue.
- The detailed Safety Concept is co-determined by the respective licensing approach and environment. This means that there is no universal Safety Concept; instead each licensing environment has its own Safety Concept. However, the basic logic of the Safety Concept is universal.
- In the following, we will deal with the Safety Concept from a top-down perspective; i.e. we do not expand on its details. A full Safety Concept would compile a lot of information and become more and more detailed during the life cycle of a nuclear facility.

After these remarks, we are offering a first approach to our definition of the Safety Concept:

- Ensuring the safety of a nuclear facility to be built, commissioned and operated is embedded into a stepwise process. The Safety Concept aims at deriving the applicable technical requirements in a systematic approach, providing for adequate processes for implementing the aforementioned requirements and demonstrating credibly that these requirements are actually achieved.
- In a first step, the applicable technical requirements governing safety need to be determined. They could e.g. be taken from the applicable codes and standards.
- In the next step, these requirements need to be implemented in the design of the plant.
- During construction and erection, the proper implementation of the design requirements introduced in the design stage needs to be verified on the hardware side. This would require appropriate processes to be considered in this part of product realisation.
- In commissioning, the achievement of at least part of the technical requirements would be verified by means of suitable tests.
- In the operation stage, the framework of the acceptable plant parameters and states would be such that they comply with the technical requirements which the plant design is based on. The achievement of this framework would be verified during operation e.g. by means of in-service inspections (ISI), review of the operation records etc.

From the aforesaid, we conclude that the Safety Concept compiles necessarily both technical and procedural requirements. The technical requirements are used as technical input to the design, the commissioning instructions, the operation instructions etc. whereas the procedural requirements govern the processes to implement and verify the achievement of the technical requirements.

It should have become credible that the Safety Concept is an integral top-down approach to ensuring that the General Nuclear Safety Objective "... *to protect individuals, society and the environment by establishing and maintaining in nuclear power plants an effective defence against radiological hazard ...*" (INSAG-12, No.: 13) is achieved. It accompanies all stages of the plant life cycle. This firstly underlines that the Safety Concept should be seen as a permanent issue in the plant life cycle and secondly makes clear that defining a conclusive and consistent Safety Concept in an early stage of the project is of utmost importance and requires a lot of attention. Irrespective of the universal features of the Safety Concept, we will in the following restrict ourselves to the life cycle stages up to commissioning. This will facilitate understanding the basic features of the Safety Concept.

3.3 Approaches to the Technical Requirements Part of the Safety Concept

Basically, there are two different approaches to derive the Technical Requirements of a Safety Concept:

- The "evaluating-the-experience-based approach": Historically, this was the way how the LWR design requirements were derived. It made use of the experience gained in previous reference project(s), be they directly comparable to the project under consideration or not. The uncertainty about the direct applicability of the reference project(s) required screening the previous experience as a must; successful application of such a process lead to requirements which usually are denoted as "General Design Criteria" or similar. The term "screening the previous experience" would include the screening of high-level design and safety requirements, like the Defence-in-Depth principle and others, with respect to applicability to the project under scrutiny. Furthermore, the inherent safety features of the plant and their due consideration in the design and safety assessment need to be determined.
The benefit of such a "good engineering practice approach" is that it is easy to perform and it does not take long to achieve the results; this implies that they are available very early in the design and safety assessment processes. This approach leads to a set of high-level design requirements which usually need to be broken down to a more detailed level. Among its drawbacks are that it is not easy – if not impossible – to quantify the safety margins, the safety significance of the General Design Criteria does not become evident or is even not justifiable and doubts/uncertainties about the completeness of these criteria derived from experience will prevail.
- The "functional analysis approach": Its main feature is a systematic analysis of the consequences of challenges to the Fundamental Safety Functions (reactivity control, heat removal and enclosure of radioactivity) which are caused by the initiating events to be considered for design and safety assessment of the specific plant. The outcome of this approach is a set of safety functions to be performed by the SSC; they can be further broken down into more detailed design requirements like system safety functions and technical requirements for each Defence-in-Depth level.
The benefit of this approach is its systematic, analytical methodology which supports credibility about the completeness of the derived design requirements, its compatibility with the safety classification and its transparency which grants an at least qualitative understanding of the safety margins. Its main drawback is its intricate nature which implies performing a time-consuming analysis before the actual design and safety assessment processes can be initiated.

Of course, the technical requirements part of the Safety Concept can also be implemented by combining the aforementioned two approaches to form a two-step process: In the first step, the generic requirements to be considered in the Safety Concept are derived. In the second step, the safety functions are determined as indicated above and further broken down into plant-specific technical requirements. They would supplement those derived in the first step and be part of a complete and consistent set of technical requirements for the design of the plant. Such a combination is advisable because certain well-established deterministic requirements which are not necessarily an outcome of the systematic analyses, like the single failure criterion. This could be based on the aforementioned "evaluating-the-experience-based approach".

3.4 Approach to the Procedural Part of the Safety Concept

Determining the technical requirements as an integral part of the Safety Concept is a process per se. This exemplifies that processes in general play a dominant role in the implementation of a Safety Concept. There are other important processes which we address in more detail in

the following. Similar to the technical requirements, the processes need to be defined beforehand and implemented at the right time in the overall process of product realisation. Other than the technical requirements, the procedural part of the Safety Concept is to a larger extent depending on the specific licensing environment in a specific country. However, there are certain procedural features which are universal to licensing; we will focus on these features.

We have identified as the main processes up to commissioning:

- Determination of the technical requirements: The respective processes are outlined above and need not be discussed in detail again.
- Safety Case preparation and basic design: This process includes inter alia design up to basic design, safety assessment thereof and preparation of the Safety Analysis Report as well as the balance of the Safety Case. For establishing the requirements in Safety Case Preparation and the associated processes, at least the following issues have to be specified to the necessary detail:
 - Scope of basic design,
 - rules for handling the basic design process,
 - requirements on safety assessment,
 - relations and interfaces between basic design and safety assessment,
 - requirements on scope and content of the Safety Case,
 - rules for review and rework of the documents comprising the Safety Case.In case that in the Safety Case preparation phase interaction with the regulator is foreseen, the rules for this interaction have to be specified accordingly.
- Detail design: The processes for detail design as well as related safety assessment during the product realisation phase and for demonstrating compliance with the safety requirements shall be implemented. The methodologies of Safety and Quality Management shall be applied to the necessary extent. For the purpose of the Safety Concept, a description on conceptual level will be sufficient. Guidance can be taken e.g. from IAEA documents INSAG-12, NS-R-1 and NS-G-1.2. Specific issues to be considered in the description are for instance the
 - basic concept of the detail design and safety assessment and verification processes,
 - identification of the roles and responsibilities of the parties involved in the processes,
 - information flow and design review,
 - approval of detail design documents,
 - procedures to be followed in design modifications,
 - feedback from safety assessment to design.
- Construction and erection: A process to demonstrate compliance of the as-built SSC with the applicable design and safety requirements during construction and erection has to be implemented under consideration of the specific licensing environment. The methodologies of Safety and Quality Management shall be applied to the necessary extent. The measures implemented for such verification shall be graded according to the safety significance of the respective SSC. The information on the aforementioned programmes has to encompass at least the
 - basic concept of the processes for verifying compliance during construction and erection,
 - identification of the parties involved in the processes,
 - responsibilities of the parties in the processes,
 - information flow and review activities,
 - approval of manufacturing documents,
 - inspections during manufacture and erection,
 - resolution of non-conformances,
 - feedback from verification of compliance to design and safety assessment.

Details of the actual process for confirming compliance can be clarified later in the licensing process; therefore, the respective description in the Safety Concept should be on conceptual level.

- Testing, qualification and commissioning (TQC) as well as code verification and validation (V&V): The processes of Testing, Qualification and Commissioning (TQC) as well as code verification and validation (V&V) are of specific significance for first-of-a-kind plants which requires extensive activities in these areas with the aim to justify the design basis and the operational procedures. Therefore, concise and representative programmes for TQC and V&V tailored to the respective reactor and duly considering the safety significance of the items foreseen for these processes have to be elaborated. The methodologies of Safety and Quality Management shall be applied to the necessary extent.

Guidance for the procedural requirements may be taken from applicable safety standards derived for the LWR; however, care has to be taken that the generic requirements are adapted appropriately to the plant under scrutiny.

The information on the aforementioned programmes has to encompass at least the

- basic concept of the TQC and V&V processes,
- method for identifying the items for TQC and V&V,
- identification of the parties involved in the processes,
- responsibilities of the parties in the processes,
- information flow and review activities,
- approval of TQC documents,
- involvement of the parties in TQC investigations,
- feedback from TQC to design.

Depending on the specific licensing environment, there might be further processes which are not addressed here. They could be added to the procedural part of the Safety Concept accordingly.

3.5 The Integral Safety Concept

When we combine the aforesaid on the technical requirements and the procedural part, we arrive at an overall Safety Concept which we have depicted in Fig. 1. In this figure, the different colours are indicating different categories of requirements or processes, respectively.

The first group of requirements – coded red in Fig. 1 – consists of the deterministically set high-ranking requirements based on experience as documented e.g. in the applicable IAEA codes and standards. They support demonstrating the achievement of the General Nuclear Safety Objective by making use of the Defence-in-Depth principle under simultaneous consideration of the inherent safety features of the plant. In doing so, a certain relaxation is introduced: The inherent safety features of the plant may be credited in design and safety assessment of the plant. Further input is taken from the Technical Safety and Radiation Protection Objectives according to INSAG-12 as well as from screening the established codes and standards for comparable state-of-the-art reactors.

The outcome of the analysis of the plant safety features and the available codes and standards described above is a set of General Design Criteria which is not necessarily complete. It should be supplemented by a systematic analysis – coded green in Fig. 1 – which after finalisation would lead to the complete list of technical requirements which are coded blue in Fig. 1.

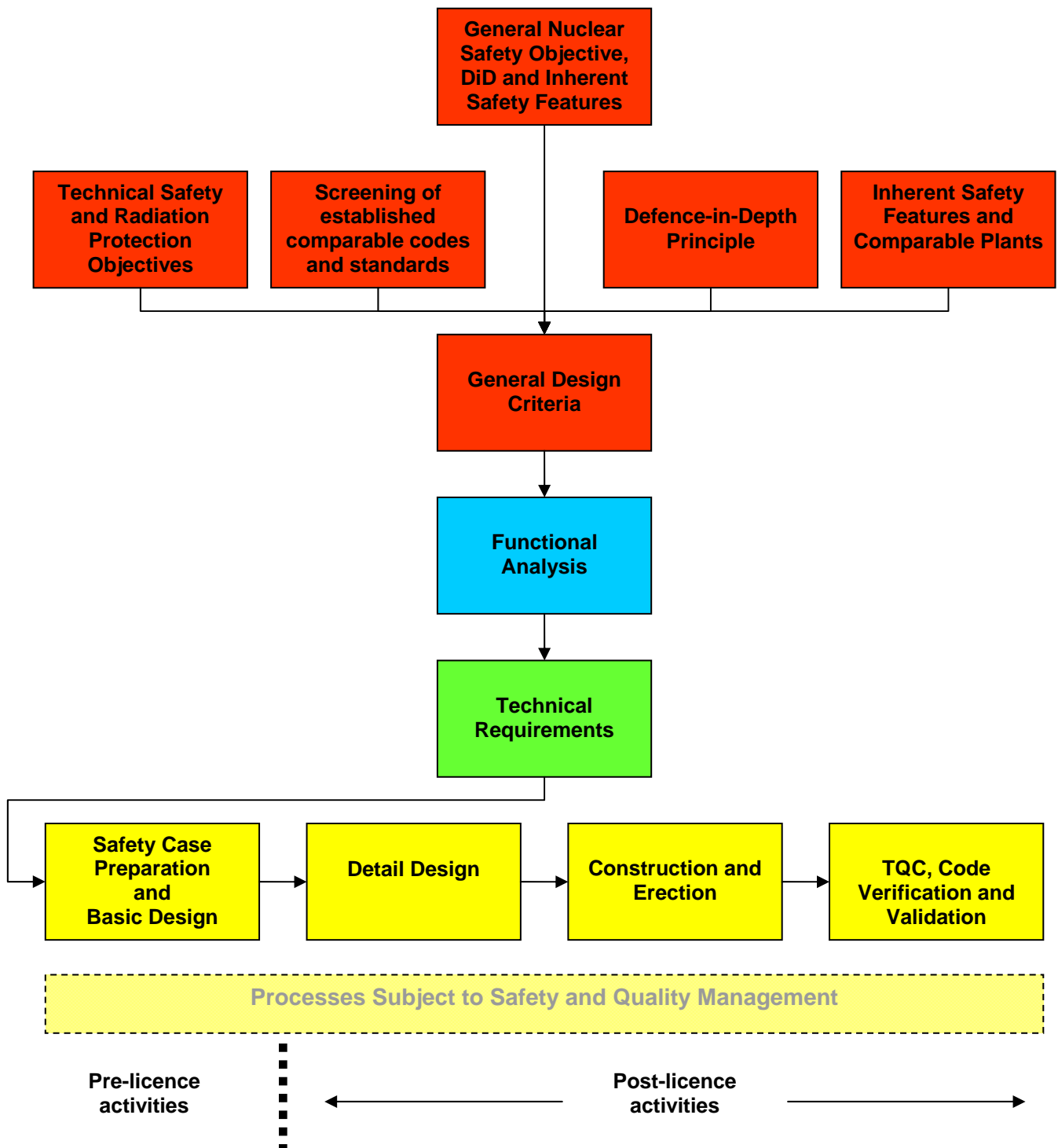


Fig. 1: The Integral Safety Concept

Once the technical requirements have been determined, the ensuing processes are:

- Safety Case preparation and basic design
- detail design,
- construction and erection,

- TQC, code verification and validation

They are coded yellow in Fig. 1. Sub-processes are not indicated in Fig. 1. All of the above processes are subject to quality and safety management. It should be self-evident that deriving the technical requirements as outlined above is also a process which we denote as “Determining the technical requirements”.

As stated already, the individual licensing processes depend on the licensing environment which is specific for each country. For this reason, we do not see a possibility to allocate the processes outlined above to a “generic licensing process”. However, as a rule of thumb, the Safety Case preparation and basic design would belong to the pre-licence activities, whereas the ensuing processes are post-licence steps.

It should be emphasised that this outline of the overall Safety Concept is only meant to be an example for implementing such a concept. Other approaches are possible and acceptable. The most important message of this presentation is to implement a Safety Concept at all, to optimise it such that it captures the actual features of the plant and to update it permanently during the life cycle of the plant. This would reduce the effort to attain a licence considerably and at the same time establish a basis for a plant design which is consistent from the safety perspective.

4 CONCLUSIONS

It should have become evident that the Safety Concept is an integral part of a pro-active licensing approach aiming at the rigorous identification and implementation of the applicable technical requirements and processes in a top-down process. Both from the technical and legal perspectives, the Safety Concept as discussed above appears to be logic, straightforward and self-evident.

There might remain the question: “What is really new about the Safety Concept and is it necessary at all? We are used to this methodology since long.” Or, in other words: Do we need the proposed Safety Concept?

Given the experience which we referred to at the beginning of this presentation, the answer is simple: Yes, we need to consider this – or a similar – methodology. Evidently, there are gaps in the contemporary approaches to attain a licence. How else would it be possible to reference findings as we did; findings which demonstrate the evident deficiencies in the respective licensing attempts? How else can we explain that for a number of projects, the safety philosophy appears to be acceptable; however, its implementation causes trouble? One might object that we referenced the wrong examples, they are specific. Such objection does not hold: From what we heard from licensing processes outside our involvement, they are featuring similar deficiencies.

If so, why not facilitate the licensing approach by means of a consistent Safety Concept?

For the sake of clarification, a few remarks should be added:

- We do not insist that our terminology and understanding of the Safety Concept is universal. Any other term might be used for denoting a pro-active approach to licensing providing for an early identification of the technical requirements and their due implementation by means of suitable processes.
- We do not claim that our approach is the only possible one. We are convinced that a number of equally feasible and acceptable approaches exist which could be credited in

licensing. The specific licensing environment plays a dominant role in the elaboration of a Safety Concept and requires due consideration.

- From a generic perspective, implementing logic as outlined above is the real issue; the details of the Safety Concept need to be fixed within the specific project only.
- Among the benefits of a consistent Safety Concepts is a reduction of the efforts in and cost of licensing.
- For all of the above, an agreement with the regulator should be established before the details of the Safety Concept are defined and implemented.

Usually, a consultant has only limited possibilities to implement a Safety Concept; this should primarily be the role of the applicant and the plant designer. However, TÜV NORD Nuclear can provide consultancy how to overcome the difficulties, deficiencies and gaps mentioned above.