PROJECTING REGULATORY EXPECTATIONS FOR ADVANCED REACTOR DESIGNS

A. Viktorov
Canadian Nuclear Safety Commission, Ottawa, Ontario, Canada

Abstract

This paper explores the overarching safety principles that will likely guide the safety design of advanced reactor technologies. As will be shown, the already established safety framework provides a solid foundation for the safety design of future nuclear power plants. As a specific example, the principle of "proven technology" is presented in greater detail and its implications for a novel technology are discussed. Research, modeling and prototyping are shown to be components in satisfying this principle.

While the fundamental safety principles are in place, their interpretation may depend both on the considered technology as well as the national context. Thus, the regulatory authority will need to be engaged, at an appropriate stage of the technology development, in specifying the regulatory requirements that will have to be met for a specific reactor design.

1. Introduction

It is said that "the overall success of the Generation IV program depends on, among other factors, the ability to develop, demonstrate, and deploy advanced system designs that exhibit excellent safety characteristics" [1]. It is also well known that demonstrating safety is not a simple task; one needs a coherent set of goals, criteria, starting with high-level safety principles, and tools, including engineering standards and analytical models. A significant effort put by the international community in defining safety principles, requirements and expectations must be acknowledged with more focus placed on harmonization of national expectations and requirements. A number of international cooperative undertakings actively contribute to leveraging of research efforts and sharing of ideas, data and breakthroughs. The most substantial ongoing endeavors for the next generation reactors include the **Generation IV International Forum GIF** [2], **International Project on Innovative Nuclear Reactors and Fuel Cycles INPRO** [3], **International Framework for Nuclear Energy Cooperation IFNEC** (formerly GNEP) [4], **Sustainable Nuclear Energy Technology Platform SNETP** (European Union) [5]. These international collaborative projects aim to:

- Enable international community to cooperate in innovations in nuclear energy systems
- Make sure that nuclear energy is available to contribute to meeting the energy needs of the 21st century in a sustainable manner,
- Identify, prioritize and carry out the research and development (R&D) needed to establish the feasibility and performance capabilities of the next generation nuclear energy systems,
- Ensure the use of nuclear energy proceeds in a manner that is efficient and meets the highest standards of safety, security and non-proliferation.

As part of these, as well as other national and international activities, a safety framework emerges to guide safety design of innovative systems, which builds on the existing mature practices but also takes a forward looking approach. The key aspects of this safety framework are discussed below.

2. Safety Principles for Advanced Reactor Designs

The fundamental safety objectives and principles - for the operating reactors and for designs that are currently being considered for construction - are well established within the nuclear industry on both national and international levels. The fundamental safety principles [6] condensed from the nuclear industry practices are in fact applicable well beyond the nuclear sector. It stands to reason that these principles, undoubtedly refined, will still be germane in several decades from now.

The fundamental principles, invaluable as they may be in setting a safety framework, are not lending themselves easily to everyday needs of a reactor designer. IAEA offers a set of guidance aimed at this level as well: **IAEA Safety Standard NS-R-1** [7] summed up hundreds of years of nuclear reactor design experience in countries with mature nuclear industries (the document in turn has given rise to a number of national adaptations). Let us quickly go over some of the higher level design principles.

Fundamental safety functions
The design shall ensure that the following safety functions can be performed with the required reliability, for the full duration of the design life:

- Control of reactivity;
- Removal of heat from the core;
- Confinement of radioactive material, and provision of shielding against radiation.

Proven engineering practices
Where a novel design or feature is introduced or there is a departure from an established engineering practice, safety shall be demonstrated to be adequate by means of appropriate supporting research programmes and performance tests with specific acceptance criteria.

Safety assessment
Comprehensive deterministic and probabilistic safety assessments shall be carried out during the design process to demonstrate that safety requirements are met throughout the plant's lifetime.

Safety and security interface
Safety measures and security measures shall be designed and implemented in an integrated manner so that security measures do not compromise safety and safety measures do not compromise security.

Defence in depth
Independent levels of defence shall be provided so that if a failure or a deviation from normal operation were to occur, it would be detected and compensated for, corrected and/or controlled.

Management system for design
Management system for assessment of the design shall be implemented in all design phases. This system includes provisions for each structure, system and component so that the quality of its design, as well as the overall plant design, is ensured at all times.

The US NRC formalized their **expectations for advanced reactors in a formal policy statement** [8], which aligns well with the IAEA principles [7] despite being directed at the design that are perhaps a decade further away than those for which the IAEA document was written. Notably, the NRC policy puts more weight on the use of less complex, inherent and passive features as well as on addressing security threats. The text of the policy statement itself is quite brief but it provides a total of 14 design attributes in addition to guidance on several other aspects. Below are given some highlights.

(Some of) Design attributes that will provide enhanced margins to safety

- Highly reliable and less complex shutdown and decay heat removal systems. The use of inherent or passive means to accomplish this objective is encouraged.
- Simplified safety systems that, where possible, reduce required operator actions, equipment subjected to severe environmental conditions, and components needed for maintaining safe shutdown conditions.
- Designs that minimize the potential for severe accidents and their consequences by providing sufficient inherent safety, reliability, redundancy, diversity, and independence in safety systems, with an emphasis on minimizing the potential for accidents over minimizing the consequences of such accidents.
- Designs that incorporate the defense-in-depth philosophy by maintaining multiple barriers against radiation release, and by reducing the potential for, and consequences of, severe accidents.
- Design features that can be proven by citation of existing technology, or that can be satisfactorily established by commitment to a suitable technology development program.
- Designs that include considerations for safety and security requirements together in the design process such that security issues can be effectively resolved through facility design and engineered security features, and formulation of mitigation measures, with reduced reliance on human actions.
- Designs with features to prevent a simultaneous loss of containment integrity and the ability to maintain core cooling as a result of an aircraft impact, or identification of system designs that would provide inherent delay in radiological releases (if prevention of release is not possible).

Other expectations

- The applicants are responsible for documentation and research necessary to support an application. Research activities include testing of new features that differ from existing designs.
- Design innovations that enhance safety and depend on proven technology are encouraged. In absence of operating experience, plans for technology development should be presented.

One statement from [8] in particular deserves a full quotation: *"Regarding advanced reactors, the Commission expects, as a minimum, at least the same degree of protection of the environment and public health and safety and the common defense and security that is required for current generation light-water reactors (LWRs). Furthermore, the Commission expects that advanced reactors will provide enhanced margins of safety and/or use simplified, inherent, passive, or other innovative means to accomplish their safety and security functions."*

This expectation would put the new reactor technologies to a tough test as the safety of the Generation III reactors is already very high[1], even though the efficiency may not be. In other words, the advantages of the new technologies in efficiency, proliferation resistance or utilization of fuel would not be sufficient, in itself, to win over the established and proven LWR technology.

Report 9 provides a very recent regulatory point of view on the key safety principles for near-future nuclear plants. A working group under **WENRA** was tasked with reviewing the existing national approaches and selecting a set of safety objectives for new reactors with the aim of promoting higher levels of safety. The "new reactors" considered in that study involve mostly the Generation III reactors that begin being build in Europe; but some "deferred plants" based on the earlier designs also needed to be taken into consideration. A set of seven safety objectives was put forward as a result; these are summarized below:

Normal operation, abnormal events and prevention of accidents

- Achieving reduced frequencies of abnormal events and reduced potential for escalation of such events to accident situations.

Accidents without core melt

- Ensuring that accidents without core melt induce no off-site radiological impact or only minor radiological impact.
- Reducing the core damage frequency and releases of radioactive material.
- Consideration of impact of all external hazards and malevolent acts.

Accidents with core melt

- Practical elimination of accidents with core melt which would lead to early or large releases.

[1] Recent OECD publication "Comparing Nuclear Accident Risks with Those from Other Energy Sources" provides some statistics to shore up this statement.

- For accidents with core melt that have not been practically eliminated, only limited measures are needed for protecting the public.

Independence between all levels of defence-in-depth

- Enhancing the independence between all levels of defence-in-depth in addition to strengthening of each level separately to provide an overall reinforcement of defence-in-depth.

Safety and security interfaces

- Ensuring that safety measures and security measures are designed and implemented in an integrated manner.

Radiation protection and waste management

- Reducing by design provisions, for all states and activities, of doses for workers, discharges to the environment, and radioactive waste.

Management of safety

- Ensuring effective management of safety from the design stage through effective leadership, and maintaining sufficient technical and financial resources .

Finally, the document [10] provides a summary of the safety philosophy and principles to be considered in the design of advanced reactor systems and the underlying R&D. Again, the philosophy and principles draw from the IAEA work but also account for the fact that the novel systems may require different approaches to achieve the desired levels of safety. The key safety principles developed in [10] can be summarized as follows:

Opportunities exist to further improve on nuclear power's already excellent safety record

The achieved level of safety is excellent and can be kept as a reference for future reactors. While not required formally, further safety improvements are possible. Such improvements should promote the "built-in" features rather then be "added on" to the system.

Safety improvements should simultaneously be based on several elements

These include risk reduction, adoption of ambitious safety goals, application of innovative technologies, emphasis on accident prevention, improved robustness of safety demonstration.

The principle of defence in depth must be preserved in the design of Generation IV systems

The design process should be "risk informed" and consider both deterministic and probabilistic methods

In addition to prototyping and demonstration, modeling and simulation should play a large role

Prototyping and demonstration are expensive and contribute to the long lead times for development of new technologies. Making use of sophisticated modeling tools and computing power can provide means of a more thorough evaluation of design features critical to safety.

The objective of this somewhat extensive summary[2] of the four significant documents setting forward-looking safety expectations [7-10] was to bring upfront the similarities and identify differences of substance in approaches. All four references build on the best modern national and international practices and offer a forward looking perspective. The shared principles that seem to be most prominent are:

- *striving for improving safety*
- *design in depth*
- *proven technology*
- *consideration of security aspects*

The differences are partly due to the different objectives or target audiences of the reports; nevertheless some nuances in the approaches may signify somewhat different views of the challenges in assuring safety of future.

Now, let us ask ourselves whether there are any reasons for the safety principles as described above to undergo a substantial transformation for technologies different from those in existence now. Several evolutionary trends come to mind that are likely to bring some differences in application of the above principles, such as

- growing use of risk-informed decision-making based on the maturing risk prognostication tools
- quickly advancing computational methods allowing modeling of phenomena previously out of reach for analysts
- gradually diminishing availability of large experimental facilities, affecting the capability to acquire direct experimental data, and even more so, the means of their independent verification
- surge in security concerns that is likely to persist in the next decades
- tighter coupling of the management techniques with all stages of design development, including the supporting research and training.

These, and other, not yet detected trends or unanticipated events, will, no doubt, lead to a refinement of the high level safety principles. However, their fundamental importance in setting the safety framework is likely to persist in the future.

[2] The author of this paper makes no claim of providing a comprehensive overview of all relevant sources. The referenced documents are comprehensive reports containing a wealth of information; out of this wealth only those elements were mentioned in this paper that help directly with highlighting the key design principles for safety for future reactors.

Finally, it would be appropriate to caution that all of the above safety principles are at a relatively high level, and as such are applicable to a wide range of technologies. However, as one works its way down to more detailed requirements on a system level, it should be expected that the specificities of various technologies will require careful consideration and adaptation to the particular needs, capabilities or challenges. Moreover, at some level of detail, the elaboration on the universally recognized safety principles will diverge due national specifics.

3. The "Proven Technology" Principle

3.1 Defining the principle

As can be seen from the preceding discussion there exist a solid basis of high level safety principles to guide a designer of a nuclear reactor. Application of the high level principles, however, is not always clear, especially for advanced reactor concepts. Let take as a case in hand the principle of "proven technologies" and consider its possible interpretation for rather novel technologies at the core of Generation IV reactor designs. Going to the authoritative source, we will find the principle stated in IAEA INSAG-12 [11] as follows:

PROVEN TECHNOLOGY: *Technologies incorporated into design have been proven by experience and testing. Significant new design features or new reactor types are introduced only after thorough research and prototype testing at the component, system or plant level, as appropriate.*

Clearly, the principle is not meant to bar the introduction of novel, advanced features or whole technologies, but then, what exactly needs to be done to satisfy this expectation? Before tackling the implication of this principle for new reactors, especially those of advanced designs, let attempt elaborating on the statement of the principle itself. Document [12] provides some recent thoughts on the subject, from the perspective of countries considering introduction of the nuclear technology. Building on those and other consideration, the following could be proposed:

a. Proving a technology involves multiple levels:
   - Individual components (equipment pieces, structures, as well as design and analysis techniques, methods and software);
   - Systems (which are composed of multiple, often diverse in nature, elements – mechanical, electrical, procedural, software, etc);
   - Overall plant; and
   - The complete technology cycle (the plant, fuel manufacturing, waste disposal) including the interface with coupled applications (i.e., desalination or hydrogen production).

b. Methods by which a technology and its components may be proven are combinations of qualification activities through testing, modeling and simulations, and experience at similar types of facilities.

c. Several degrees of proof of a technology on the level of the overall plant could be distinguished:
   - Initial "licensability" level – a prerequisite for obtaining a licence or certification in the country of the technology origin. At this level, no operating experience at the plant level could yet be available, but the combined proof from operating experience of similar technologies, qualification activities and analytical evaluations should be sufficient to allow construction and operation of a prototype or first of a kind plant;
   - Intermediate level – corresponding to experience accrued through several years of operation at the first of a kind or prototype facility;
   - Mature level – with successful experience shown by several plants over years of operation with good record.

d. As part of the process of "proving" a technology, dedicated provisions should be made to document the experience, starting from qualification activities and simulations, to the operation of the first of a kind facility, to the experience with the operation of multiple plants. Similarly, critical evaluations of the technology, including those by the regulatory agencies, should be documented. These provisions will capture the objective evidence.

e. Utilization of "proven engineering practices[3]" should be treated as an essential element supporting the principle of "proven technology". When there are no applicable standards due to the substantial novelty of the technology, those engineering practices, methods, approaches, etc that were applied, should be codified as the national or international standards following the systematic process.

3.2 Benefits of "proven technology"

Having discussed what is implied by the "proven technology" principle, we will turn now to the benefits offered by adhering to this principle, especially with respect to the safety of the public.

In general, the "provenness" of a technology allows reducing business risks to the licensee; at the same time it also allows more accurate gauging and management of safety risks posed to the public.

Very briefly, on the business side:

a. Investment risk is better understood and controlled with the technology that has been shown to operate successfully.
b. Scheduling risks are minimized with the available experience in manufacturing and construction of identical or similar facilities.
c. An operating organization is more easily set up if it can draw assistance from other utilities already operating similar facilities.

[3] NS-R-1 [7] defines a principle of "Proven Engineering Practices" which can be concisely stated as "the design shall be in accordance with the relevant and approved engineering standards and codes".

d. Operational and technological "glitches" are fewer in number and faster addressed as experience with operation grows and is shared among the "technology-owners group" .

These benefits are so substantial that the "provenness" of technology often becomes a utility requirement. On the other hand, the regulatory authority would apply this principle with the view of its safety advantages. As the safety benefits offered by a proven technology are of primary interest to us, here is a somewhat more elaborate discussion:

e. Points (b), (c) and (d) stated above are not only of economic benefit but are also attractive from the safety point of view. Accumulated manufacturing and construction experience not only allows speeding up the process but improves quality; the operating experience assist in promoting the safety culture and benefitting from established operational, maintenance, inspection, etc., processes.

f. The "provenness" of a technology involves systematic identification of safety concerns posed by, or to, the technology. An appropriate knowledge base and simulation capability are developed enabling demonstration that the safety concerns are addressed in design. Essentially, the process of "proving" the technology goes hand in hand with demonstration that such fundamental safety principles as defence-in-depth, safety assessment, prevention of accidents, are satisfied.

g. From the regulatory point of view, the technology is "proven" when there is enough understanding of it, built from objective evidence, that allows prediction with high confidence of both the likelihood of safety challenges and of their consequences.

3.3 "Proving" an advanced technology

When an innovative technology is being developed, naturally there would be no operating experience and, at the beginning, limited knowledge of least some aspects. Novel features, improvements that go beyond the established standards or practice need to be brought to the level of 'proven technology' through appropriate evaluation, qualification, testing and/or prototyping. Quoting from NS-R-1 [7]:

> *Where an unproven design or feature is introduced or there is a departure from an established engineering practice, safety shall be demonstrated to be adequate by appropriate supporting research programmes, or by examination of operational experience from other relevant applications. The development shall also be adequately tested before being brought into service and shall be monitored in service, to verify that the expected behaviour is achieved.*

A technology demonstration program must be developed to facilitate the introduction of a technology, featuring:

- identification of components and systems that require proving;
- identification of operational and safety challenges to select the range of conditions for evaluation

- planning and execution of an R&D program both to directly test components as well as to collect data for developing analytical tools
- development of analytical tools, such as models, correlations, computer simulation capabilities, and their subsequent validation
- development of engineering practices, and their codification as standards
- documentation and sharing of experience and data
- cooperation of the involved parties.

3.4 Roles of prototyping, testing and analytical "proof"

The six technologies included in Generation IV framework are all significantly different from the mainstream water-cooled reactor technology of the currently operating reactors. In effect this means that the scope of technology elements that require proving is quite large.

Prototyping would seem as the ultimate proof of a technology or its element – but from the safety perspective its value could be questioned. Here is why:

> Firstly, to build a prototype nuclear reactor (meaning, most likely, scaled down in power rating) it must be licensed and be shown to satisfy the same stringent safety requirements as "regular" plant. This means that the proof by testing and modeling must be already in place.
>
> Secondly, the technology cannot be tested in a prototype facility to demonstrate its performance under accident conditions. Hardly anyone would trigger a large break loss of coolant accident in a nuclear reactor to see how well safety systems will perform and how much damage the fuel would suffer[4].

On the other hand, prototyping may well have great benefit from the operational point of view allowing ironing out wrinkles in design and operation of the process systems.

The technology proof by necessity occurs before the first, either pilot or full-scale, plant is built. This is achieved through a prudent combination of basic single-effect tests to study phenomena and acquire knowledge, development of sophisticated modeling tools, and integral tests to both qualify the technology elements and validate the tools; all this topped where possible with demonstration of technology elements in similar facilities.

The theoretical understanding of phenomena, robustness of models, coupling of various physical disciplines in computer codes used in design and safety demonstration of advanced reactors are expected to exceed that what is in existence these days. In particular,

- challenges to safety functions and physical barriers should be identified and studied with the objective of firmly establishing safety and failure limits for each challenge and each barrier;

[4] One might recall that the RBMK reactors operated for several decades of reactor-years without any significant mishap – and thus could have claimed to be a proven mature technology. Then the Chernobyl accident happened and demonstrated that design was not adequate from the safety perspective.

- models and correlations are established over the full range of conditions and the associated uncertainties are quantified; normally that would require that high-quality experimental data are available from several independent, different scale experimental set-ups;
- an integral evaluation methodology should be created to allow modeling of the whole plant and its behavior in transients and accidents. While it is acceptable to use separate qualified codes, they should be able to run together when important feedback effects exist;
- regardless of the availability of advanced simulation tools, the key safety components need to be demonstrated by tests, most of all in cases where interaction of several components is important.

No matter in what exactly way the technology and its components are proven, this would require time, expertise, investment and availability of experimental facilities, as well as a concerted effort to bring together numerous stakeholders. In particular, the need to experimentally demonstrate technology elements may require a long lead time. It only makes sense to take careful stock of the available facilities to get assurances that the experimental base is adequate for technology demonstration or to initiate building of new experimental rigs if required. International cooperation becomes hugely important in this context.

3.5 Some of SCWCR technology challenges

Let us finally dwell on some of the features of super-critical water cooled reactor technology that would require demonstration of mastering of the potential safety challenges.

- Reactivity effects of the super-critical (in the thermodynamic sense!) core should be studied to prove the stability of power control in normal conditions and transients.

- Design, optimization and analysis of the reactor coolant system heat transfer in transients and accidents. Effectiveness of the heat removal with the single phase coolant must be demonstrated for transients such as loss of coolant, loss of flow, loss of pressure control, etc.

- Durability of materials for the primary coolant system and core components, subjected to the typical conditions over the full plant life duration will have to be proven. Aging and degradation mechanisms accounting for the chemistry and irradiation effects, must be identified and addressed.

- Appropriate limits and criteria need to be established for the identified challenges to all safety functions and barriers, taking into account conditions that may exist in design basis and beyond design basis events.

- Any passive or simplified features in the design of reactor and its safety systems need to be shown to provide adequate protection against challenges and threats.

The examples given above are widely acknowledged as areas requiring attention and substantial R&D efforts. However, it would be wrong to build an R&D strategy on ad-hoc list of issues. The designer is expected to apply a systematic process as part of the technology demonstration program to assure that the reactor and plant systems are "proven" for the range of conditions, and the tools used in design and safety analysis are validated.

Finally, it would be of course wrong to think that the technology or its elements need to be "proven" for the sake of a check-mark against this principle. Test, experiments, assessments, models and, where possible, demonstration in a similar facility, are all parts of building up comprehensive safety assessment, which integrates knowledge and objective evidence, and provides confidence in the technology.

4. Concluding Thoughts

As has been shown in this paper, the high level safety principles are available to guide the R&D, assessment and design of future nuclear systems. These principles build on the successful record of enhancing safety of Generation III fission reactors; by incorporating lessons learned certain aspects are adjusted to better suit the future expectations. Some differences exist and will likely to continue to exist in interpretation of those high level principles, driven by both the national regulatory regimes and specifics of chosen technologies. Nevertheless it is important to continue harmonization efforts to reduce the cost of development and licensing of reactor system in various jurisdictions.

We also explored in some detail the meaning of the "proven technology" principle for novel, advanced reactor technologies, showing that the proof would involve balancing of the three core activities, such as experimental programs, development of modeling capabilities and prototyping. It is important to remember that a complex technology can only be partially predictable – primarily due to an almost infinite number of permutations in the ways that the technology elements, and outside factors, can interface. However, by "proving" a technology, a conscious effort is made to identify the credible safety challenges and to predict likely consequences. It is also important to recognize that meeting this principle should not be an isolated effort – it is closely interlinked with fulfilling other safety principles, such as defense in depth, comprehensive safety assessment, use of deterministic and risk-informed insights, etc.

Finally, I would like to point out that researchers and designers probably would not think much of involving a regulatory agency in assessments of a reactor design, which is 20 or 30 years away from being ready for licensing. But as a design takes shape, it only makes sense to start a dialogue with the regulator. Quite early on in the design, it will be necessary to define, in addition to the performance requirements, the safety requirements as well. As experience shows, the new technology always necessitates a fresh look at the safety framework and brings about changes in the existing regulatory expectations to accommodate specific features of the technology. Some regulatory requirements may have a substantial impact on the basic design – i.e., core reactivity feedback effects, requirements for safety systems, need to have well supported safety criteria, etc. A timely dialogue with the regulator reasonably early on in the design, allows

- Reducing / managing regulatory risk – improved predictability and benefit for competitiveness
- Preparation of the needed licensing framework which takes into account specifics of the technology
- Developing engineering standards that will form part of the proven engineering practices.

5. References

[1] "Basis for the Safety Approach for Design & Assessment of Generation IV Nuclear Systems", Revision 1, 2008, NEA GIF/RSWG/2007/002.
[2] http://www.gen-4.org
[3] http://www.iaea.org/INPRO
[4] http://www.gneppartnership.org
[5] http://www.snetp.eu
[6] "Fundamental Safety Principles", IAEA SF-1.
[7] "Safety of Nuclear Power Plants: Design", IAEA NS-R-1.
[8] "Policy Statement on the Regulation of Advanced Reactors", NRC-2008-0237-0010.
[9] "Safety Objectives for New Power Reactors", WENRA, 2009.
[10] "Basis for the Safety Approach for Design & Assessment of Generation IV Nuclear Systems", Revision 1, 2008, NEA GIF/RSWG/2007/002.
[11] "Basic Safety Principles for Nuclear Power Plants", 75-INSAG-3. Rev 1, INSAG-12. IAEA, 1999.
[12] "Common User Considerations (CUC) by Developing Countries for Future Nuclear Energy Systems: Report of Stage 1", IAEA Nuclear Energy Series No. NP-T-2.1 2009.