Risk-informed graded approach for regulatory oversight of nuclear facilities

Jan-Erik Holmberg[a], Ari Julin[a]
[a]Radiation and Nuclear Safety Authority, Vantaa, Finland

Abstract:

The purpose of grading is to allocate available resources in an optimal manner. The safety standards of the International Atomic Energy Agency (IAEA) expect that graded approach is to be applied in the management of the regulatory oversight, beginning from the legislation and regulation down to practical arrangement of regulatory activities. Risk is a fundamental consideration in determining which level of regulatory controls are to be applied. The term "risk-informed graded approach" addresses this aspect of graded approach, and it is based on use of insights from probabilistic risk analysis to support grading of oversight activities.

In the Finnish nuclear safety regulatory system, risk-informed approach in the regulatory oversight is promoted. To utilize the insight from probabilistic risk analyses, dedicated plant-specific tools, called RIGA (risk-informed graded approach), have been developed at Radiation and Nuclear Safety Authority in Finland (STUK). RIGA accounts for both the functional risk importance (single failure and common cause failure) and the importance of loss of structural integrity of components. The functional risk importance is obtained from nuclear power plant specific PRAs, while the importance of loss of structural integrity is assessed in risk-informed in-service-inspection applications. This paper presents STUK's graded approach for regulatory oversight of nuclear facilities, including the RIGA tool.

Keywords: Graded approach, risk-informed regulatory oversight, PRA, PSA

1. INTRODUCTION

IAEA Safety and Security Glossary [1] defines the graded approach for a system of control, such as a regulatory system or a safety system, a process or method in which the stringency of the control measures and conditions to be applied is commensurate, to the extent practicable, with the likelihood and possible consequences of, and the level of risk associated with, a loss of control. As such, this safety principle is generally followed in the safety management of nuclear facilities all over the world. As an example, the safety classification of structures, systems and components (SSC) sets the quality assurance requirements for the design, manufacturing, installation, operation and maintenance of the items of nuclear installations.

Although the risk informed graded approach can be regarded as an obvious principle to optimize the allocation and use of regulatory resources, its practical implementation is far from self-evident. Among other things, the challenges lie in the difficulty to objectively assess the safety importance of an item as well as in the plurality of items (targets of the regulatory oversight) that are subject to grading. The scope of grading does not only cover SSCs but also various safety-related activities, processes, documents, events, etc., during the whole life cycle of the system such as a nuclear facility.

In the Finnish nuclear safety regulatory system, risk-informed approach in the regulatory oversight is promoted. It means, e.g., use of insights from probabilistic risk analysis (PRA) to support grading of oversight activities. One cornerstone of the approach used by Radiation and Nuclear Safety Authority in Finland (STUK) is the newly developed RIGA (risk-informed graded approach) tool. RIGA accounts for risk importance metrics obtained from nuclear power plant specific PRAs. This paper presents STUK's graded approach for regulatory oversight of nuclear facilities, and the properties of the RIGA tool.

2. APPLICATION OF RISK-INFORMED GRADED APPROACH AT STUK

2.1. General scope and expectations for graded approach

Generally, when applying graded approach in the management system for a product, item, system, structure or component, service, activity or controls of a process, the significance for safety, health, environmental, security, quality or economic aspects are assessed [2]. In this context, the consideration is limited to risks of nuclear energy and radiation risks, which are the primary concern of a radiation and nuclear safety authority.

The graded approach has been included in the Finnish legislation in such a way that the risks associated with different types of facilities and activities have been considered in the regulatory control and in safety requirements for organizational parties. According to Finnish Nuclear Energy Act (990/1987) Section 7a [3] “The safety requirements and measures for ensuring safety shall be graded and targeted so as to be commensurate with the risks in the use of nuclear energy”.

Graded approach has been systematically implemented in STUK’s oversight processes, which was also notified by the IAEA Integrated Regulatory Review Service (IRRS) Mission Team in 2022 [4]. With reference to the IAEA GSR Part 1 (Rev. 1) [5], STUK’s model for overall safety management of nuclear installations was regarded as a good practice by the IRRS Mission Team. IAEA GSR Part 1 (Requirement 26, paragraph 4.46) states that “For an integrated safety assessment, the regulatory body shall first organize the results obtained in a systematic manner. It shall then identify trends and conclusions drawn from inspections, from reviews and assessments for operating facilities, and from the conduct of activities where relevant. Feedback information shall be provided to the authorized party. This integrated safety assessment shall be repeated periodically, with account taken of the radiation risks associated with the facility or activity, in accordance with a graded approach”.

2.2. Regulatory oversight processes of nuclear facilities

STUK’s regulatory oversight processes of nuclear facilities are divided into four groups: 1) licenses and approvals, 2) assessments, 3) inspections, and 4) implementation and enforcement.

Licenses and approvals include oversight of plant projects (new-builts, plant modifications), handling of license applications for nuclear materials and nuclear waste, oversight of the transport of nuclear material and nuclear waste, personnel approvals and organizational approvals. From the grading point of view, large plant projects belong to the highest grade as such, but for the other types of approvals it is relevant to consider grading of use of resources.

Assessments cover a wide range of safety, security and safeguards assessments of facilities, systems, structures, materials, processes and components. Use of graded approach is highly relevant for these oversight processes, but the grading often requires consideration of several aspects (see chapter 2.4 for further discussion).

The inspections performed by STUK are divided into inspections according to inspection programmes, compliance inspections and nuclear material inspections. Application of graded approach is relatively straight forward since it can be related to the safety importance of the inspected targets. Safety classification of the item is one of the criteria, but it is not the only criterion (see chapter 2.4 for further discussion)

The procedures used in implementation of official requirements are based on the authorisations granted to the authorities in legislation. The choice of procedure, i.e., grading, to be used in any given situation is primarily based on the safety importance of the situation or matter requiring rectification. It is usually straightforward to choose the appropriate procedure, but there can be similar complexities as with assessments.

2.3. Nuclear safety classification

Safety classification is a specific type of grading applied to Structures, Systems and Components (SSCs) or to activities. It is a method of grouping items with similar characteristics or functions for the purpose of identifying appropriate requirements, codes, and standards to be applied to their design, manufacture, construction, operation and maintenance.

It could be noted that there are several classifications in use at nuclear facilities. Most important one is the ”nuclear safety classification” required by the nuclear safety regulation. STUK’s regulation on the safety of a nuclear power plant [6] states that “the safety functions of a nuclear facility shall be defined, and the related systems, structures and components classified on the basis of their safety significance. In addition, requirements set forth and the actions taken to ascertain the compliance with the requirements of the systems, structures and components implementing safety functions and connecting systems, structures and components shall be commensurate with the safety class of the item in question”.

In the Finnish system, SSCs shall be grouped into the Safety Classes SC1, SC2 and SC3 and Class EYT (non-nuclear safety) based on their significance for the implementation of safety functions [7]. SC1 corresponds with the nuclear reactor cooling circuit (primary circuit). SC2 includes safety systems designed to cope with postulated accidents to bring the facility to a controlled state and to maintain this state. In addition, containment isolation function belongs to SC2. SC3 includes a variety of safety related systems, e.g., system designed to bring the facility into a safe state after anticipated operational occurrences, postulated accidents, and design extension conditions as well as severe accident management systems.

Nuclear safety classification is mainly based on deterministic safety assessments, but risk-based adjustments shall be considered, too. In principle, safety classes could be used as one of the primary means to the graded approach, but this approach has several limitations. Firstly, it is oriented to SSCs, while regulatory oversight has many other orientations and targets, too. Even when applied to SSCs, the deterministic safety importance takes into account risk importance in a limited manner. Secondly, safety classification is a static way of grading and does not consider the regulatory decision-making context. As a conclusion, STUK’s internal guide for review and assessment has been developed to compensate the limitations of safety classification system (see next chapter).

2.4. STUK’s internal guide for graded approach in regulatory oversight of nuclear facilities

STUK’s internal guide for graded approach defines the oversight process to address all known factors that could impact on the nuclear safety risk, or the radiation safety risk caused by a subject whenever deciding on any oversight measures relating to that subject. Herein, ‘subject’ means a facility’s technical structures, systems and components as well as operating processes and procedures.

The grading process leads to the determination of the subject’s regulatory oversight review class (RC), which is one the following:

- RC1: full-scale oversight
- RC2: focus on most important aspects
- RC3: focus on conclusions or spot checking
- No review by STUK.

The determination process has the following steps:

1) Choice of the determination approach
2) Grading of the subject depending on the chosen determination approach (preliminary grading).
3) Consideration of factors that can upgrade or downgrade the review class (final grading).

The guide provides three approaches to the determination of the safety importance: 1) based on the impact of the subject to the defence-in-depth concept of the facility, 2) based on PRA results (risk-informed graded approach) and 3) direct approach. In addition to these approaches, there are a few application-specific determination approaches defined in corresponding internal guides, e.g., related to radiation protection, security management, and nuclear waste management.

The impact of the subject to the defence-in-depth concept of the facility follows the deterministic importance of the subject. Depending on the safety class of the item and its functional role in the defence-in-depth concept of the facility, there are tabulated rules to choose the review class. For instance, if the subject concerns with a system that fulfils safety function related to design basis accidents, it receives the preliminary grade RC1.

The risk-informed graded approach is described in detail in the next chapter.

The direct approach simply suggests the preliminary grade RC2, which is a typical choice in many cases.

The preliminary grade can be upgraded or downgraded if there are other context-dependent factors not taken into account in the preliminary grading. The guide provides a list of typical factors. Examples of upgrading factors include first-of-a-kind (FOAK) subject, deficient safety assessment by the licensee and recurring event. Examples of downgrading factors include updating of an earlier accepted documentation and a known subject without any previous deviations.

3. RIGA TOOL

3.1. General concept

RIGA tool is an information system for grading of SSCs and events based on risk information from plant-specific level 1 and 2 PRA and risk-informed-in-service-inspection (RI-ISI) application. With regard to SSCs, two risk importance measures are used:

- Functional risk importance = risk increase factor (RIF) if the item is not operable This risk metric is obtained from the level 1 and 2 PRA, considering both reactor core damage and fuel damage in spent fuel pool.
- Structural risk importance = conditional probability of reactor accident if the structural integrity of the item is lost. This risk metric is obtained from the plant-specific RI-ISI application, where risk importances of pipe segments are quantified.

In RIGA, SSCs are classified in five risk importance classes w.r.t. both functional risk importance and structural integrity criticality (Table 1).

Table 1. Risk importance classes of RIGA.

Class	Risk importance
1	High
2	Medium
3	Low
4	Very Low
5	Not in PRA/RI-ISI

The review class depends on the safety class and risk importance class (Table 2). The review class is mainly equal to the risk importance class, except when the risk importance is very low or when the item is not in PRA or in RI-ISI.

Table 2. Determination of review class based on risk importance class and safety class.

Risk Class	RIF	CCDP	CLRP	Safety class			
				SC1	SC2	SC3	Non-nuclear safety
1	RIF ≥ 11	1E-4 –	1E-5 –	RC1	RC1	RC1	RC1
2	2 ≤ RIF ≤ 11	1E-5 – 1E-4	1E-6 – 1E-5	RC2	RC2	RC2	RC2
3	1.1 ≤ RIF ≤ 2	1E-6 – 1E-5	1E-7 – 1E-6	RC3	RC3	RC3	RC3
4	1 ≤ RIF ≤ 1.1	– 1E-6	– 1E-7	RC3	RC3	RC3	No review
5	Not in PRA/RI-ISI			RC1	RC2	RC3	No review

RIF = Risk increase factor
CCDP = Conditional core damage probability (or fuel damage probability in spent fuel pool)
CLRP = Conditional large release probability

For components, not only single failure RIF values are applied but also RIF values of associated common cause failures (CCFs) are considered. The reason for this is that the regulatory task is often not only related to a single component but to a set of similar components.

In the determination of system's risk importance, the maximum risk importance metric of components in the system is applied.

The structural importances of components are determined by the structural importance of piping segment (as evaluated in RI-ISI application), if applicable. The structural importance is relevant to pump, valve, tank, heat exchanger type of components.

In the evaluation of events, CCDP and CLRP are used as risk metrics.

Risk classes are defined both for 1) an average plant operating state (POS), 2) power operation POS and 3) shutdown POS. The shutdown POS represents average risk over all shutdown related plant operating states.

3.2. Tool development and maintenance procedure

There are RIGA tools for each nuclear power unit in Finland: Loviisa 1 and 2, and Olkiluoto 1, 2 and 3. The database has been developed combining risk information from plant-specific PRA models and RI-ISI application with the component location catalogues of each unit, i.e., lists of SSCs at the unit.

The main effort in the development of the tools has been to associate relevant location to each location related basic event defined in the PRA model. Usually, the location can be directly identified from the basic event ID, but there is also a need to manually check those basic events whose ID does not follow component location ID based designation system.

Concerning CCF events, all locations corresponding with the CCF event need to be identified. Usually, these can be directly identified from the CCF event groups defined in the PRA model, but PRA model can also include CCF events whose content has not been explicitly defined in the model (but is explained in the documentation). High redundant component groups are typical examples of such CCFs.

An important task is to identify possible system configuration assumptions, which may cause asymmetries in the PRA model, for instance, assumptions related to system trains in operation/standby, and impacts of hazards only to selected system trains. Asymmetries can cause that redundant system trains do not receive equal risk importance metrics even if they are equally important. Such biases must be corrected.

In Finland, the licensees update PRA models annually and submit the models to STUK for notification. The RIGA tools are updated accordingly. The updating of RIGA tools is relatively simple, depending naturally on the extension of updates in PRA. In any case, all changes in risk classes need to be checked to identify the reason for changed class. First versions of RIGA were available in 2022, meaning that the tools have been updated 1–2 times after that for all nuclear power plant units.

3.3. Applications

RIGA tools are intended to be general supporting tools for any inspector at STUK. Two applications have been developed for dedicated purposes.

One of STUK's task is to supervise the licensee, manufacturers, inspection and testing institutions and, to the extent necessary, other parties in order to ensure the safe operation of the nuclear facility and to carry out the inspections required by the regulatory guides, in which the compliance of systems, equipment and structures is assessed. A specific RIGA application has been developed to support the grading of inspections and reviews of mechanical equipment of nuclear facilities in connection with the design, manufacturing, installation and commissioning of a nuclear facilities and in in-service periodic inspections of pressure equipment. The rules to determine the review class are the same as in Table 2. This RIGA tool contains a list of component locations, associated mechanical safety classes, risk classes and review classes and this information is integrated in the inspection database system used by the inspectors to document the inspections.

Regulatory oversight during the operation of the nuclear facility includes frequently assessments of risk importance of events or system and component unavailabilities. It can be important to be able to assess the risk significance in a timely manner, so that additional information can be requested in due time. Therefore, another RIGA application has been developed which provides component location, system and event importances graded based on risk classes as in Table 2. The plant operating state (all, power operation or shutdown) is distinguished in the database. This database gives the first insight of the risk importance, but in more complicated cases PRA experts should be involved in the assessment.

3.4. Limitations

Same uncertainties as in PRA and RI-ISI are applicable to RIGA. On the other hand, when RIGA is maintained and used by several users, it can raise valuable questions revealing possible biases or flaws in PRA models. RIGA can be thus also considered a process that supports STUK's review of plants' PRA models.

PRA models include several simplifications for which reason location specific risk metric can be difficult to find. For instance, screening of events can leave out components for which risk increase factors could be high. It is also typical to model fault tree basic events that merge several components or even represent a whole system. Definitions for CCF events may be sometimes ambiguous. Also, asymmetry assumptions related to the modelling of certain initiating events and system configurations cause bias in the results. If this kind of simplifications are not properly documented, the risk importances of associated components are missed.

System configuration assumptions used in PRA should be properly documented to identify whether redundant components should receive same risk class even though their risk importances could be different. Inevitably, there are cases, where seemingly redundant system trains do not have same functional risk importance, in which a judgement is needed to decide whether redundant component location should receive same risk class or not.

If a component has a risk importance close to the class limit (e.g. RIF is close to 1.1), it can happen that the class changes when the PRA model is updated, even if there has practically been no change in the risk importance of that component. Such changes may be experienced undue by the users, and therefore they should be avoided. There could be a need to implement a hysteresis property in RIGA, but this is an open issue, so far.

4. CONCLUSION

Graded approach is a safety management principle that nuclear safety regulators are expected to follow in all regulatory activities. Concerning oversight of nuclear facilities, the safety classification of SSCs often provides the first approach to grading, but it has several limitations. It does not fully take into account the risk importance and it does not address contextual factors.

STUK's internal guide for risk informed regulatory oversight of nuclear facilities has been developed to compensate the limitations of grading based solely on safety classification. Three approaches for the determination of the review classes are defined: 1) based on the impact of the subject to the defence-in-depth concept of the facility, 2) based on PRA results (risk-informed graded approach) and 3) direct approach. The preliminary grade can be upgraded or downgraded if there are other context-dependent factors not taken into account in the preliminary grading.

To facilitate the risk-informed grading, plant-specific tools called RIGA has been developed. Tools are based on plant-specific level 1 and 2 PRA models and RI-ISI applications. RIGA tools make the PRA information easily available for non-PRA experts by providing risk classes of SSCs. Two RIGA applications have been further developed: 1) grading of inspections of mechanical equipment, 2) risk assessment of operational events. Quality of RIGA is dependent on the quality of PRA model and documentation.

References

[1] IAEA Nuclear Safety and Security Glossary, International Atomic Energy Agency, Vienna, 2022.

[2] Use of a Graded Approach in the Application of the Management System Requirements for Facilities and Activities, IAEA-TECDOC-1740, International Atomic Energy Agency, Vienna, 2022.

[3] Finnish Nuclear Energy Act (990/1987).

[4] Integrated regulatory review service (IRRS) mission to Finland, IAEA-NS-IRRS-2022-09, International Atomic Energy Agency, Vienna, 2022.

[5] Governmental, Legal and Regulatory Framework for Safety, General Safety Requirements Part 1, No. GSR Part 1 (Rev. 1), International Atomic Energy Agency, Vienna, 2016.

[6] Radiation and Nuclear Safety Authority Regulation on the Safety of a Nuclear Power Plant, STUK Y/1/2018, Radiation and Nuclear Safety Authority, Helsinki, 2018.

[7] Guide YVL B.2. Classification of systems, structures and components of a nuclear facility, 15.6.2019, Radiation and Nuclear Safety Authority, Helsinki, 2019.