International Conference on Topical Issues in Nuclear Installation Safety:
Defence in Depth – Advances and Challenges for Nuclear Installation Safety
Vienna, 21 to 24 October 2013

The Design Options and Provision File and the role of the defence in depth within the pre-licensing of the MYRRHA project

G.L.Fiorini[1]; N.Hakimi[1]; B.Tombuyses[2]; C. Dams[2],
A.Wertelaers[2], M. Schrauben[2], R. Dresselaers[2]

1 – Nuclear Safety Consultant on behalf of FANC
2 – Federal Agency for Nuclear Control (FANC), Belgium

FANC
federal agency for nuclear control

Introduction

- The SCK-CEN MOL is designing MYRRHA (Multi-purpose hybrid research reactor for high-tech applications), an irradiation facility considered as a Gen-IV technology (50-100 MW_{th});
- MYRRHA is conceived as an ADS, able to operate in sub-critical and critical modes.
- It comprises a proton accelerator of 600 MeV, a spallation target and a multiplying core with MOX fuel, cooled by liquid lead-bismuth.
- The installation should be operational at full power around 2023

Role of the FANC

- The Belgian Federal Agency for Nuclear Control (FANC), in accordance with the procedures specified within the RGPRI*, shall deliver the permission for the construction and the operation.
- The documents to be submitted to FANC include, among others, the description of the installation, the technology retained by the applicant for the facility and a Preliminary Safety Report.
- For MYRRHA a pre-licensing process, whose details are defined by FANC, is implemented to follow the pre-project.

** RGPRI - Arrêté royal du 20 juillet 2001 portant règlement général de la protection de la population, des travailleurs et de l'environnement contre le danger des rayonnements ionisants*

Documents issued by FANC

As part of this pre-licensing action, documents issued by the regulator are organized in a hierarchical manner:

- a Strategic Note identifies safety goals, safety objectives, regulations and standards applicable to the project;
- the Design Options and Provision File (DOPF) template for a set of volumes, which will be prepared by the designer, whose main objective is to organize the presentation and the discussion with FANC;
- a series of thematic Guidances will describe in more detail the expectations of the regulator, in relation to the project (e.g. on earthquake, aircraft crash, etc.).

Role of the Defence in Depth

- The Defence in depth (DiD) and its fundamental principles remain the foundation of the whole process described by the Strategic Note and materialized by the DOPF.
- The DiD principles shall be fully implemented for the design of MYRRHA and it will be, among others, on the basis of compliance with these principles that the concept will be assessed.
- The designer attention is drawn on the availability of recent references – e.g. from WENRA - which formulate proposals for refinements of the concept of DiD, as well as recommendations on how to incorporate these refinements within the design.

FANC
federal agency for nuclear control

The MYRRHA Strategic Note - Objectives

The objectives of the Strategic Note are summarized as follow:

- to recall and resume the regulatory framework applicable to MYRRHA project (Class 1 nuclear facility);
- to present and motivate the safety, security and safeguard philosophy;
- to shortly present and motivate the content of the Design Options and Provisions File (DOPF) which incorporates both the "*Dossier d'options de sûreté (DOS)*" and the "*Dossier d'options de sécurité*"

The Safety Philosophy

- The safety philosophy includes the information necessary to translate the safety principles, requirements and guidelines into safety options and into design and operational specifications which are needed to select the technical and operational provisions (e.g. equipment and operational procedures, etc.);
- High-level safety goals and objectives are developed into quantitative targets for use by the designer.

The Safety Philosophy (cont.)

Safety Principles, Requirements and Guidelines

- Safety Fundamental Principles are defined by IAEA Safety Standards.
- IAEA (and others) requirements are available; they are not systematically fully applicable to new installations like MYRRHA. A specific effort can be needed to adapt or develop specific documents to finalize the regulatory framework.
- Several IAEA Safety Guides provide recommendations and guidance on how to comply with the IAEA safety requirements.
- Taking into account the specificity of MYRRHA, other complementary guidance documents may be followed, provided a justification is presented.

The Safety Philosophy (cont.)

Safety goals and safety objectives

- Internationally endorsed safety goals and objectives, applicable to a hybrid research reactor, are not yet available.
- Following FANC, for MYRRHA, the expected level of safety should:
  - reach, as a minimum, a level as high as the level of the (best) installations, according to the WENRA objectives for new nuclear power plants
  - tend to the highest level that can be expected for new reactor designs – i.e. the Generation IV safety goals

The Security and Safeguards Philosophy

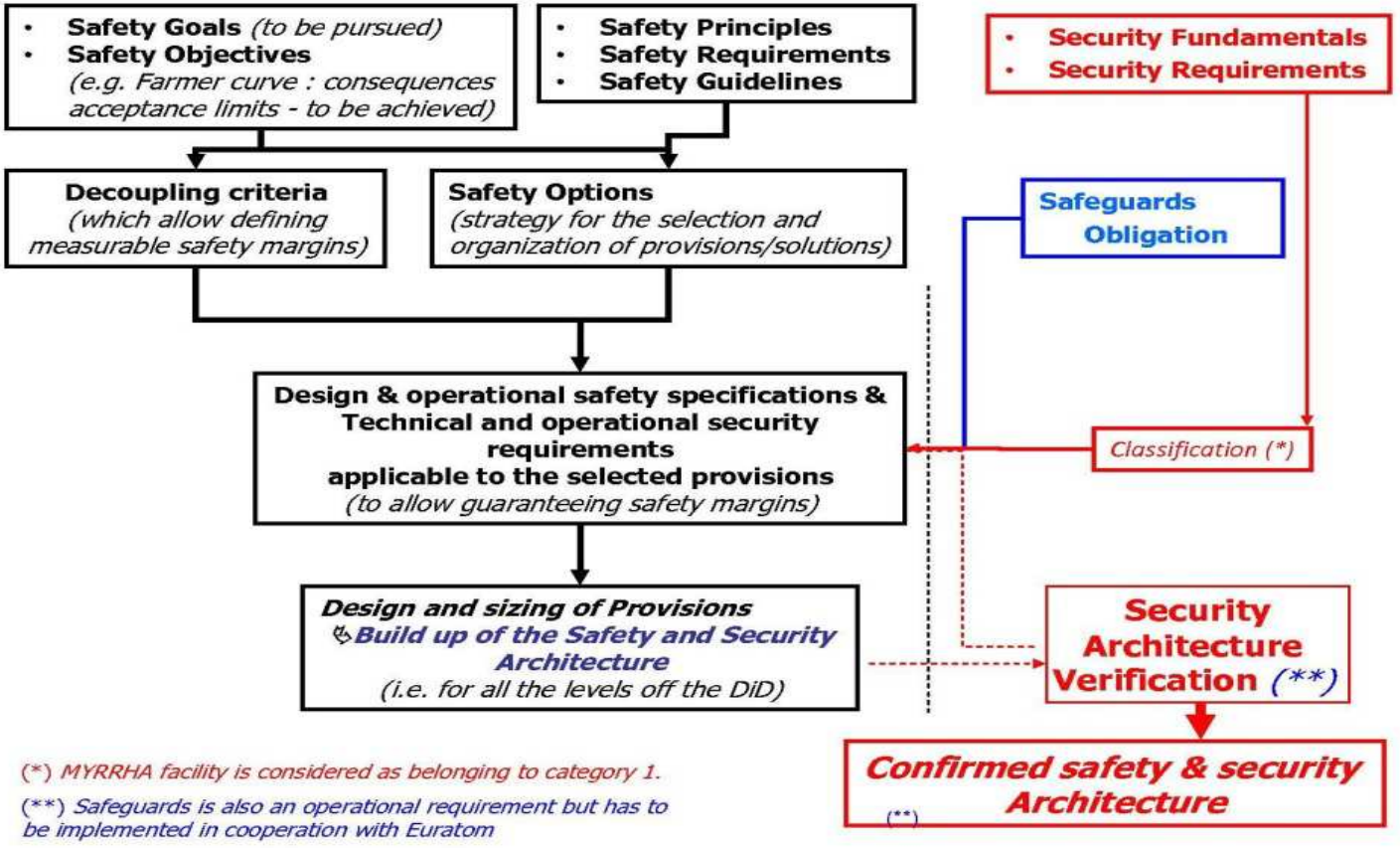
- The security philosophy is based on objectives, principles and requirements.
- The objectives stress the need to prevent, detect, delay and intervene in case of malevolent event.
- The twelve fundamental security principles cover: *Responsibility of the State; Responsibilities During International Transport; Legislative and Regulatory Framework; Competent Authority; Responsibility of the License Holders; Security Culture; Threat; Graded Approach;* ***Defence in Depth****; Quality Assurance; Contingency Plans; Confidentiality.*
- These principles are the basis of the regulation concerning the physical protection and will lead to the security requirements which motivate the need for the identification and categorization of Design Basis Threat (DBT)

Design Options and Provisions File (DOPF)

Within the DOPF the designer will present:

- the selected safety and security provisions implemented within the design,
- the operational safety specifications as well as the technical and operational security requirements, taking into account the safeguards obligations.
- the safety design and operational specifications are themselves derived from the safety options proposed by the designer.
- The DOPF will also provide indications about the measures implemented to approach the safety goals and to achieve the defined safety objectives.

DOPF Flowchart



Logic and links between the different steps for the design and the safety / security pre-licensing assessment

FANC
federal agency for nuclear control

DOPF Template

A top tier template is proposed by FANC for the DOPF; it is organized in different volumes to ease the presentation and the analysis:

- *Volume 1: Purpose and description of the facility;*
- *Volume 2: Approach to the nuclear safety;*
- *Volume 3: Design Options and selected provisions and their justification against the objectives, goals, principles, requirements and guidelines;*
- *Volume 4: Management system for safety of the installation;*
- *Volume 5: Security and Safeguards Integrated Approach*

The objectives for the different volumes and the concatenation within the DOPF

Objectives of the volume 1 :"Purpose and description of the facility"

- to present the description and characteristics of the site;
- to present the installation both in terms of its overall architecture and the description of its different components;
- to provide information on operation modes;
- and finally to present the interactions of the plant with its environment.

Estimations of the potential source term for the different plant conditions (normal and abnormal) should also be indicated.

➢ The level of detail will be compatible with the stage of the design.

The objectives for the different volumes and the concatenation within the DOPF (cont.)

Objectives of the volume 2 :"Approach to nuclear safety"

- The key objective of the volume 2 of the DOPF is to describe, discuss and motivate the safety goals, objectives, principles and the general design requirements selected by the designer and applicable to the safety architecture of the installation, considering its specificities.

- The designer shall demonstrate that the safety principles, requirements and guidelines are adequately translated into safety options and, further, into design and operational specifications, to achieve a design that will be able to fulfil the safety functions and both meet the objectives and tend towards the goals.

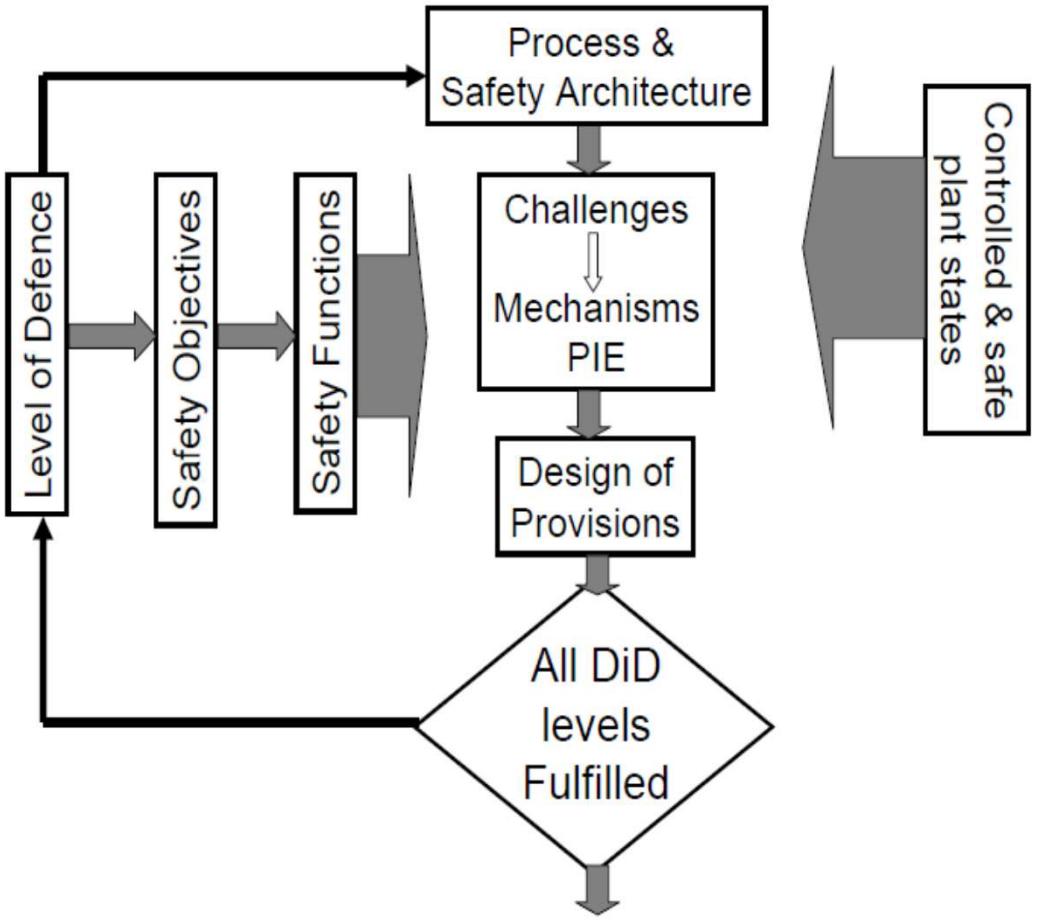
Volume 2: Approach to nuclear safety

- **Approach and steps of the design process**
  - ***Implementation of the principles of defense in depth***

Levels of defence in depth	Objective	Essential means	Radiological consequences	Associated plant condition categories
Level 1	Prevention of abnormal operation and failures	Conservative design and high quality in construction and operation, control of main plant parameters inside defined limits	No off-site radiological impact (bounded by regulatory operating limits for discharge)	Normal operation
Level 2	Control of abnormal operation and failures	Control and limiting systems and other surveillance features		Anticipated operational occurrences
Level 3 (1) 3.a	Control of accident to limit radiological releases and prevent escalation to core melt conditions (2)	Reactor protection system, safety systems, accident procedures	No off-site radiological impact or only minor radiological impact (4)	Postulated single initiating events
Level 3 (1) 3.b		Additional safety features(3), accident procedures		Postulated multiple failure events
Level 4	Control of accidents with core melt to limit off-site releases	Complementary safety features(3) to mitigate core melt, Management of accidents with core melt (severe accidents)	Off-site radiological impact may imply limited protective measures in area and time	Postulated core melt accidents (short and long term)
Level 5	Mitigation of radiological consequences of significant releases of radioactive material	Off-site emergency response Intervention levels	Off site radiological impact necessitating protective measures(5)	-

WENRA / RHWG : refined structure of the levels of DiD

Volume 2: Approach to nuclear safety (cont.)



Iterative process for the construction of the safety architecture integrating DiD principles

FANC
federal agency for nuclear control

The objectives for the different volumes and the concatenation within the DOPF (cont.)

Objectives of the volume 3
"Design Options and selected provisions and their justification against the objectives, goals, principles, requirements and guidelines"

- to show how the safety approach presented in volume 2 is implemented within the MYRRHA design (safety options, design and operational specifications, provisions) and
- to present the justification of the compliance / consistency of the design on one side versus the principles, requirements, guidelines and, on the other side, versus the goals and objectives.

➢ An essential corollary to the justification, is the proof of the feasibility of the safety demonstration in terms, for example, of available qualified tools (including codes and standards), adequate R&D support, adequate knowledge, skills and resources.

The objectives for the different volumes and the concatenation within the DOPF (cont.)

Objectives of the volume 4
"Management system for safety of the installation"

- The objective of Volume 4 of the DOPF is to present the management system in connexion to safety aspects of the installation during the project phase as well as during the operation of the installation.

➢ The management system defines: the needed level of quality, the means to achieve and maintain this quality, the means to verify this achievement and maintenance and, finally, the means to analyse and resolve possible discrepancies.

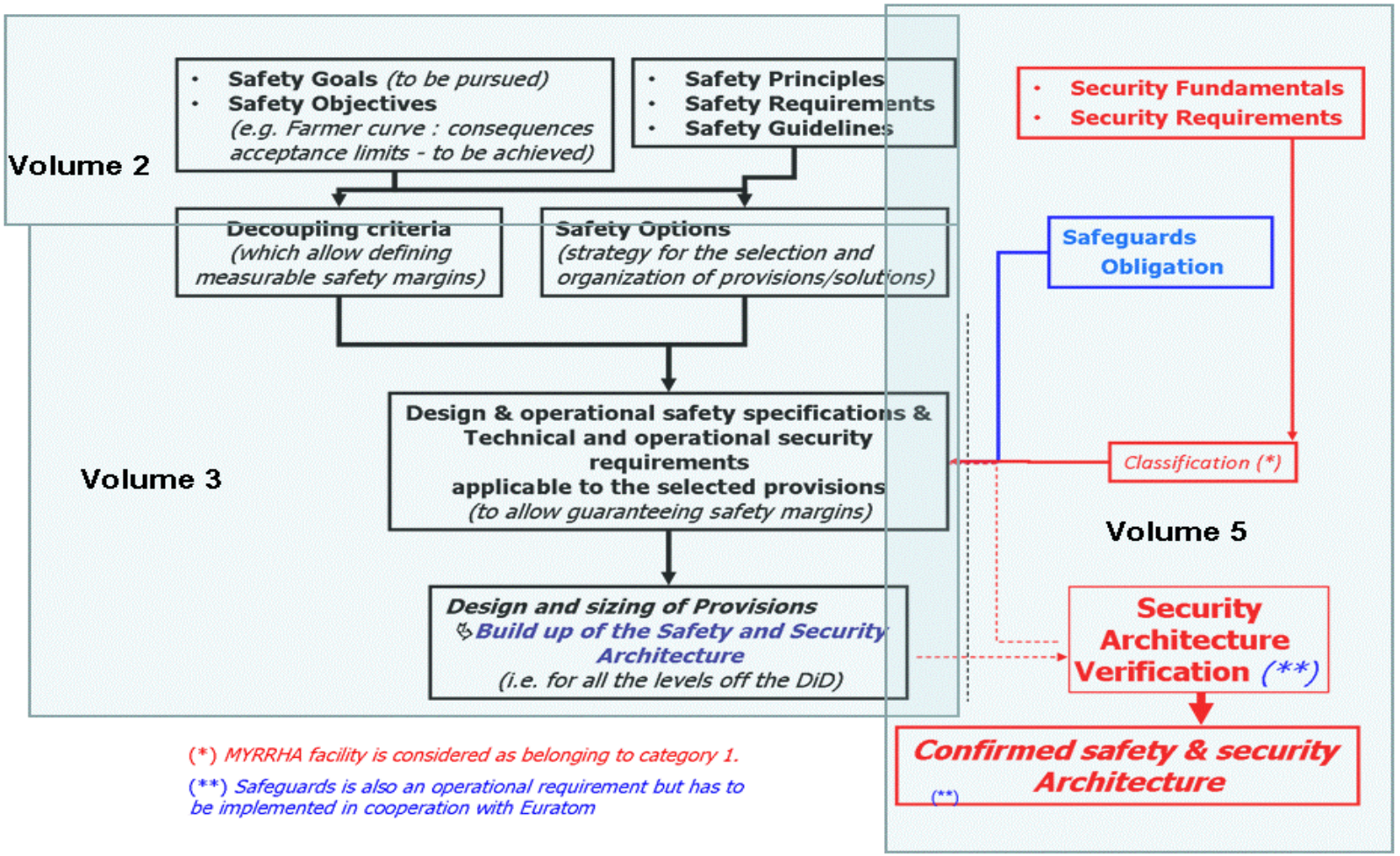
The objectives for the different volumes and the concatenation within the DOPF (cont.)

Objectives of the volume 5 "Security and Safeguards Integrated Approach"

- to recall the security fundamentals, requirements and safeguards obligation;
- to present the detail of the implementation of the provisions important to security;
- to justify the categorization of the facility;
- to present the detail of all the security measures in respect with the categorization of the facility and the site specific DBT;
- to present information that allows Euratom to set the needed measures;
- to argue that the security measures taken don't jeopardize the safety of the facility; to present the part of the management system dealing with security;
- to present the provisions taken to satisfy the safeguards obligation.

➢ In parallel, an adequate methodology should be presented to prove that, coherently with the WENRA objective O5, "*safety measures and security measures are designed and implemented in an integrated manner*".

The concatenation among the DOPF volumes



Content and concatenation for the volumes 2, 3 and 5 of the DOPF

FANC
federal agency for nuclear control

Conclusions

- FANC is engaged in a process of pre-licensing for the experimental reactor MYRRHA.
- A Strategic Note details the applicable regulatory framework.
- The Design Options and Provision File (DOPF), whose template has been prepared by FANC, is submitted by the designer to describe the steps implemented to design the installation in order to ensure compliance with the requirements of nuclear safety, security and safeguards.
- As a generic background, the DiD represents a pillar for both Strategic Note and the DOPF template.
- The two documents focus more specifically on aspects relating to refinements in the concept of DiD and on practices for their integration in the process of design / assessment of the MYRRHA reactor.

- Back up slides

FANC
federal agency for nuclear control

Volume 2: Approach to nuclear safety (cont.)

IAEA Glossary	**Plant States**					
	Operational States		Accident Conditions			
			Within Design Basis Accidents		Beyond Design Basis Accident	
	Normal Operation	Anticipated Operational Occurrences	Accident conditions that are not Design Basis Accidents as explicitly considered but which are encompassed by them	Design basis Accidents	Beyond Design Basis Accidents without significant core degradation	Severe Accidents
WENRA Proposal	**Plant Conditions categories**					
	Normal Operation	Anticipated Operational Occurrences	DID Level 3a - Postulated Single Initiating Events		DID Level 3b - Selected Multiple Failures including possible failures or inefficiency of safety systems involved in DiD level 3a	Postulated Core Melt Accident (short and long term)
EUR	**Plant Conditions**					
	Design basis Categories				Design Extension Conditions	
	1st	2nd	3rd	4th		
	Normal Operation	Incidents	Accidents (low frequency)	Accidents (very low frequency)	Complex Sequences	Severe Accidents

Categorization of the "plant conditions" or "plant states" used for the design

Volume 2: Approach to nuclear safety (cont.)

Volume 2 also discusses

- ***Stages of the design process***
- ***Principles for selecting design options and sizing provisions for the different levels of the DiD***
- ***Rules for plant's operation***
- ***Crosscut themes for the design***

FANC
federal agency for nuclear control

Volume 2: Approach to nuclear safety (cont.)

Design and operational safety specifications and criteria for nuclear safety

- The presentation of detailed design and operational safety specifications is not the primary purpose of the DOPF.
- Such request is only limited to most important safety relevant provisions (e.g. barriers) to illustrate and assess the feasibility/demonstration.

The concept of safety architecture and the Objective Provision Tree (OPT)

- The safety architecture is the set of provisions/layers of provisions that are set-up by the designer to: ensure the achievement of tasks allocated to the process in satisfactory conditions of safety; prevent the degradation of the facility
- The Objective Provision Tree (OPT) is a tool that can help during the iterative approach of definition / design of the safety architecture.

Volume 3
"Design Options and selected provisions and their justification against the objectives, goals, principles, requirements and guidelines"

The following items are developed within the Volume 3 :

- Design options and selected provisions for nuclear safety and radiation protectio;
- Identification of initiating events and their categorization into "plant states";
- Design options and selected provisions for nuclear safety;
- Design options and selected provisions for radiation protection;
- Summary table of design options and design provisions;
- Justification of the design options and selected provisions against the goals, objectives, principles, requirements and guidelines (Safety assessment);
- Design and operational safety specifications;
- Feasibility of safety analyses.

FANC
federal agency for nuclear control

Volume 3
"Design Options and selected provisions and their justification against the objectives, goals, principles, requirements and guidelines" (cont.)

Volume 3 also discusses

- **Deterministic safety demonstration**
- **Events considered to occur and consequences considered in the design**
  - *Analysis of postulated single initiating events*.
  - *Analysis of postulated multiple failure events without core melt*.
  - *Analysis of core melt accidents.*
- **Events which have to be practically eliminated, as they would lead to large or early radioactive release**

FANC
federal agency for nuclear control