

**FUNDAMENTALS OF  
SAFETY MANAGEMENT SYSTEMS  
IN NUCLEAR POWER PLANTS**

**June 2004**

## CONTENTS

<b>1</b>	<b>Preface</b>	<b>1</b>
<b>2</b>	<b>General</b>	<b>2</b>
2.1	Aim of the 'Fundamentals'	2
2.2	Procedure for preparing the 'Fundamentals'	2
2.2.1	State of the art in science and technology	2
2.2.2	Methodology	5
2.3	Area of application	6
<b>3</b>	<b>Requirements for a safety management system and for the necessary structures and elements</b>	<b>6</b>
3.1	General requirements for safety management systems	7
3.1.1	General requirements	7
3.1.2	Documentation requirements	8
3.2	Management responsibility	10
3.2.1	Management commitment	10
3.2.2	Safety requirements	11
3.2.3	Definition of the safety policy	11
3.2.4	Establishment of safety objectives	11
3.2.5	Management by setting examples	12
3.2.6	Definition of the organisational structure	12
3.2.7	Communication	13
3.2.8	Top management review of the safety management system	14
3.3	Management of the necessary resources	15
3.3.1	Provision of resources	15
3.3.2	Human resources	15
3.3.3	Infrastructure	16
3.3.4	Work environment	17
3.3.5	External organisations	17
3.3.6	Specialist competence in key areas	17

3.4	Work realisation	18
3.4.1	Planning of work realisation	18
3.4.2	Determination of the requirements for process execution and the process results	19
3.4.3	Design and development	19
3.4.4	Purchasing	21
3.4.5	Materials management	22
3.4.6	Execution of work	22
3.4.7	Control of monitoring and measuring devices within the framework of the work realisation	23
3.5	Measuring, analysis and improvement	23
3.5.1	General	23
3.5.2	Monitoring of safety performance and processes	24
3.5.3	Treatment of inadequate process results	24
3.5.4	Internal audits	25
3.5.5	External audits	25
3.5.6	Improvements	25
3.5.7	Corrective actions	26
<b>4</b>	<b>Definitions</b>	<b>27</b>
<b>5</b>	<b>References</b>	<b>30</b>

# 1 Preface

Apart from reliable technology, the operational management of a nuclear power plant is also a highly important factor to ensure safe operation. Owing to the liberalisation of the electricity markets and the resulting pressure of cost experienced by the utilities, the importance of operational management is growing since cost savings in i. a. the areas of personnel and organisation bring with them a cut in the number of personnel together with changes in the organisational structure and tighter working processes.

Experience with accidents in other branches of industry also shows the importance of safe operational management.

Today, effective safety management is seen as one crucial element of safe operational management. According to the Atomic Energy Act (*Atomgesetz* - AtG) and the Act on the Convention on Nuclear Safety, the licensee is responsible for the safety of the plant he operates. To fulfil the conditions associated with this responsibility, the licensee's company has to impose on itself an effective safety management system that complies with the requirements of the current regulations and with international standards /3, 4/.

The term safety management subsumes the entirety of all activities relating to the planning, organisation, management and supervision of individuals and work activities with a view to the efficient achievement of a high degree of safety performance, i. e. the achievement of a high quality of all activities that are important to safety, and to the promotion of a highly developed safety culture. Safety management is not limited to certain organisational units but comprises the entire safety-related organisation of the company. Safety management is the responsibility of the management level of a company.

The German nuclear regulations contain specific requirements, but no comprehensive methods or requirements for safety management. Consequently, at present there is no safety management system in place in German nuclear power plants. The licensees, however, are by now making great efforts to develop and implement safety management systems.

This results in the need to develop corresponding 'Fundamentals' in which the requirements for safety management systems are systematically compiled according to a national standard.

The 'Fundamentals' in hand contain a compilation of generally applicable features for safety management systems that are not based on a specific organisation, organisational structure or certain work processes. These 'Fundamentals' rather more provide general conditions to be adhered to in the specific structuring of the safety management systems of the individual companies and plants.

Specific requirements will be put in more concrete terms in further documents at a later stage.

The requirements for safety management systems formulated in these 'Fundamentals' do not represent a restriction of the functions and powers of the nuclear supervisory authorities.

## **2 General**

### **2.1 Aim of the 'Fundamentals'**

These 'Fundamentals', prepared as a basis for uniform nationwide implementation, contains primarily the requirements for all essential elements of the safety management systems implemented by German nuclear power plant licensees.

### **2.2 Procedure for preparing the 'Fundamentals'**

#### **2.2.1 State of the art in science and technology**

The German nuclear regulations do not contain any explicit requirements for comprehensive safety management nor for structuring the organisation under the aspect of nuclear safety that would allow the comprehensive planning and review of a safety management system. However, a number of sometimes rather general individual requirements to be fulfilled by a safety management system can be derived from the German nuclear regulations. Examples are the Radiological Protection Ordinance /1/ and the Guideline on Technical Qualification /2/.

A comparatively complete list of requirements for safety management systems can be found in the IAEA Safety Guide No NS-G-2.4 /3/ and in INSAG-13 /4/. Safety Guide No NS-G-2.4 also contains requirements resulting from a safety-related point of view for the organisational and managerial structure. In addition, NS-G-2.4 lists requirements for safety-relevant tasks that go beyond the degree of detail of these 'Fundamentals' for safety management systems.

According to INSAG-13, safety management has to be considered as being a part of quality management. Today, the requirements for quality management systems are largely contained in the EN ISO 9000:2000 ff standards. The currently used term of quality management, as it forms the basis i. a. for the EN ISO 9000:2000 ff standards, clearly means more than just the auditing at the end of a process. Other than quality assurance, quality management represents a comprehensive approach to generate high quality in a methodical manner and to constantly enhance the level of quality. Correspondingly, it has to be ensured that the requirements that result from the need for safety are fulfilled by safety management as a partial aspect of quality management. Against this background it is appropriate and expedient to build up and introduce safety management and the associated safety management system on the basis of the EN ISO 9000:2000 ff standards. In this context, the specific requirements of nuclear safety, as they are found especially in the IAEA Safety Guide No NS-G-2.4 and in INSAG-13 but also in the German nuclear laws and regulations, have to be considered.

One important stipulation in Safety Guide No NS-G-2.4 and in INSAG-13 is that one has to strive for the continual development and improvement of safety. This means that apart from meeting the demands of EN ISO 9001:2000, the corresponding requirements of EN ISO 9004:2000 also have to be fulfilled.

Safety management systems are also demanded in several other conventional branches of industry. Examples are the chemical and the petrochemical industry, where legal regulations for safety management systems exist already. The fundamental requirements for safety management systems for the chemical and the petrochemical industry can be found in the Seveso II Directive of the European Communities /5/, which entered into force in 1996 and was implemented in German law in the Hazardous Incidents Ordinance under the Federal Immission Control Act /6/ in the year 2000. This act stipulates a safety management system to prevent accidents and limit their consequences. According to /6/, the particular part of the general

monitoring system that comprises the relevant influencing parameters in connection with the definition and application of the concept for the prevention of accidents has to be integrated in the safety management system. This includes the corresponding organisational structures, areas of responsibility, ways of behaving, methods, processes, and resources. According to /6/, the safety analysis report as well as the safety management system have to be reviewed every 5 years or if there have been any safety-relevant modifications to the operating range, to a procedure or to an amount of hazardous material, or if new knowledge has been gained (e. g. from accidents).

In conclusion, the sources mentioned above provide the following common fundamental features of a modern safety management system:

- The safety management system represents a comprehensive aid to achieving, assuring and improving on a high quality of all activities that are relevant to safety.
- The safety management system represents an integral part of the quality management system and the integrated management system. It thus follows that the delimitation and the interfaces as well as the combined action and the interaction of the safety management systems with other management systems must be suitably defined and regulated.
- Within the framework of safety management, the company has to plan, organise, manage, control and supervise the numerous interconnected safety-relevant work processes. The view today is that a process-based approach has to be applied.
- The closed management cycle usually applied in management systems is to be applied to the processes covered by the safety management system; this cycle mainly consists of the elements "planning of the relevant activities" (Plan), "ordering the activities to be carried out", i. e. managing and controlling (Do), "monitoring of the implementation and the results" (Check) and "taking actions", i. e. initiating corrective and improving measures (Act).
- The safety management system has to be appropriately documented.
- The safety management system has to be reviewed at appropriate intervals and additionally if new knowledge is gained (e. g. lessons learnt from experience and from accidents) and has to be updated if necessary.

### **2.2.2 Methodology**

The "Fundamentals for Safety Management Systems" in hand are based on the EN ISO 9000:2000 ff standards. The structure of these 'Fundamentals' is oriented on the EN ISO 9001:2000 standard. The requirements of the EN ISO 9000:2000 ff standards for quality management systems to achieve a high quality of all activities relevant for the company's success were adapted by analogy, with the degree of detail of the 'Fundamentals' in hand, to the objectives of the safety management system "Ensuring the necessary safety", or more precisely "Performance of all activities relevant to safety with the requisite high quality". The degree of detail of the requirements in standards EN ISO 9001 and 9004, however, partly go beyond the degree of detail of the 'Fundamentals' in hand.

The requirements thus obtained were compared with the requirements for safety management systems of the international nuclear regulations, the detailed rules in the German nuclear laws and regulations as well as with the requirements for safety management systems in the conventional area; where it was necessary, corresponding modifications were applied.

As regards the international nuclear regulations, above all the publications of the IAEA, especially the requirements for a safety management system compiled in Safety Guide No NS-G-2.4 and in INSAG-13 were considered. The requirements for safety management systems that can be derived from the ISO 9000:2000 ff standards were compared with the requirements in Safety Guide No NS-G-2.4 and in INSAG-13 and checked for contradictions as regards content. The requirements in EN ISO 9000:2000 ff on the one hand and in Safety Guide No NS-G-2.4 and in INSAG-13 on the other hand set different priorities in several points. The requirements in Safety Guide No NS-G-2.4 and in INSAG-13 that go beyond the requirements formulated in EN ISO 9000:2000 ff were adopted. Contradictory requirements between EN ISO 9000:2000 ff and the international nuclear regulations considered were not found.

Existing rules from the German nuclear laws and regulations, such as the requirements for organisation ensuing e. g. from the Radiological Protection Ordinance /1/, the Guidelines on the Demonstration of the Technical Qualification of Nuclear Power Plant Personnel /2/, /7/ and the KTA Safety Standard 1201 "Requirements for the Operating Manual" /8/, are binding requirements that have to be fulfilled in the development and implementation of a safety management system. In the same way,

the requirements for the elements of safety management systems that can be derived from the German nuclear laws and regulations and which are relevant at the degree of detail of the 'Fundamentals' were identified and taken into consideration in the preparation of the 'Fundamentals'. Requirements contradicting the requirements of EN ISO 9000:2000 ff were not found.

In addition, the Requirements for a Safety Management System were compared with the requirements for safety management systems laid down in the existing legal regulations for the chemical and petrochemical industry (Hazardous Incidents Ordinance /6/, Appendix III). The requirements listed here coincide with the requirements made in general for management systems. There are no contradictions with the requirements of EN ISO 9000:2000 ff and of Safety Guide No NS-G-2.4 and INSAG-13, nor do any additional requirements ensue.

### **2.3 Area of application**

The 'Fundamentals' in hand contain the framework of requirements to be made for the systematic structure and completeness of safety management systems that are already in place or are yet to be implemented by the German nuclear power plant licensees. It deals with the requirements for the organisation, organisational provisions, and safety-relevant processes.

The 'Fundamentals' demand the development of quantitative target values describing safety performance but do not prescribe any such quantitative target values. Furthermore, the 'Fundamentals' make requirements for the necessary measures to promote and maintain a strong safety culture but again prescribe no values for the level to be achieved.

## **3 Requirements for a safety management system and for the necessary structures and elements**

The essential requirements for comprehensive safety management as well as for the structures and elements necessary for the implementation of a comprehensive and systematic safety management systems are presented in the following.

### **3.1 General requirements for safety management systems**

#### **3.1.1 General requirements**

- The company has to plan, develop, document, implement, maintain and continually improve an effective safety management system.
- The introduction, maintenance and improvement of the safety management system is the task and responsibility of the company's top management and has to be coordinated by the latter.
- The safety management system is to be considered as being an integral part of the quality management system and the integrated management system. Correspondingly, the delimitation and the interfaces as well as the combined action and the interaction of the safety management system with other management systems must be suitably defined and regulated.
- The safety management system has to cover all activities that may have a direct or indirect influence on safety. This includes activities that generate a high level of safety performance, activities to monitor and improve safety performance, and activities that are necessary to prevent or control anomalies, incidents and emergencies. This furthermore includes activities that are relevant not only to safety but also to other business objectives.
- The safety management system has to consider not only the nuclear power plant with its organisations and processes but also other relevant areas of the company (as far as they comprise safety-relevant tasks and responsibilities, such as the provision of resources and personnel planning) and the interfaces with external parties.
- The safety management system is to be based on a process-oriented approach for the portrayal and review of the company's work processes. This process-based approach has to comprise the following elements:
  - Identification of all safety-relevant processes and description of their purpose. Here, gaps and double regulations have to be identified and eliminated. Apart from the processes that have a direct influence on safety, the safety-relevant processes also include those processes that have an indirect influence on safety, such as management processes and supporting processes.

- Determination of the sequence and interaction of the processes in the overall system.
- Determination of methods and criteria for the operation and control of the safety-relevant processes.
- Ensurance that the sequence and interaction of the processes is devised in a way that desired results can be obtained effectively and efficiently.
- Guaranteed provision of resources and information to ensure the operation and monitoring of the safety-relevant processes.
- Routine monitoring, measuring and analysis of the safety-relevant processes with the aim to maintain and improve safety performance. An important instrument to do this is to use measurable indicators that can provide up-to-date information about the status and especially about a deterioration of safety performance.
- Determination of suitable measures for the continual improvement of the safety-relevant processes.
- The company has to ensure that safety-relevant processes that are performed outside the company are controlled and monitored for their effectiveness. Such outsourced processes have to be included in the overall context of other processes with which they interact, and the interaction of these processes has to be controlled. The core competences necessary to assume responsibility for safety and the responsibility to supervise outsourced processes must remain with the company.

### **3.1.2 Documentation requirements**

- The safety management system has to be formally documented. The documentation should be hierarchically structured. The documentation has to include the following points:
  - declaration of the company's safety policy,
  - safety objectives to fulfil the policy,
  - safety management manual,

- description of the processes and responsibilities to meet the safety objectives,
  - management's expectations for the individual processes with regard to safety (standards and targets for process execution and process results),
  - written instructions for the execution of processes and activities (process and work instructions),
  - records to demonstrate conformity with the requirements and the effectiveness of the safety management system.
- The degree of detail of the documentation has to be adapted to the importance of the safety-related regulations.
  - The safety management manual has to contain the following – if necessary in the form of an integrated management manual:
    - the area of application of the safety management system;
    - the methods devised for the safety management system. Alternatively, reference to corresponding documents can be made;
    - the interactions of the processes of the safety management system. Furthermore, the interactions and the interfaces with as well as the delimitations to other management systems have to be described.
  - It has to be ensured that the personnel has access to the documentation.
  - Safety-relevant documents (e. g. instructions for the execution of safety-relevant activities) have to be checked and quality-assured before they are issued. For this purpose, a documented procedure has to be established that takes into account the requirements of KTA 1401 /9/ and 1404 /10/, especially with regard to
    - the ensurance of an approval procedure for the individual documents that is adequate to their importance,
    - the unambiguous identification of documents,
    - the updating of documents,
    - the marking of modifications and the revision status of documents,
    - the ensurance of the availability of the relevant versions of applicable documents at their respective points of use,

- the ensurance of legibility and ready identification,
  - the identification and controlled distribution of external documents to their respective points of use,
  - the prevention of the unintended use of obsolete or invalid documents.
- The company's personnel have to be made aware of the existence of documents that are relevant from a safety-related point of view, especially after they have been updated or modified.
  - A documented procedure has to be established to ensure the storage, protection, and retrieval of documents and to ensure the retention times of records.

## **3.2 Management responsibility**

### **3.2.1 Management commitment**

- The company's management is committed to develop and implement a safety management system and to continually improve the effectiveness of the safety management system. The management has to provide evidence that it is committed to this responsibility and has to
  - establish a clear safety policy that shows the company's self-obligation for a high level of safety performance,
  - ensure that safety performance targets and safety objectives are established,
  - conduct management reviews (cf. 3.2.8),
  - ensure the availability of sufficient resources to guarantee the implementation of the safety policy.
- The company's management continually has to convey to the personnel the importance of safety and the importance of fulfilling legal and official requirements.
- The company's management has to set an example of and actively support safety-oriented acting in order to
  - strengthen and promote safety culture,
  - continually improve the company's safety performance.

### **3.2.2 Safety requirements**

- The company's top management has to ensure that external and internal safety requirements are determined, clearly defined and fulfilled (see also Chapter 3.4.2).

### **3.2.3 Definition of the safety policy**

- The safety policy has to be seen as being an integral part of the company's overall policy and strategy.
- The safety policy has to be demanding but also realistic and credible; it has to contain the following statements:
  - Safety has priority over all other business objectives.
  - The company commits itself to continually develop its safety requirements in line with the state of the art in science and technology.
  - The company commits itself to fulfilling the requirements of safety management.
  - The company commits itself to a high level of safety performance.
  - The company commits itself to continually strive for an improvement of the effectiveness of safety management.

### **3.2.4 Establishment of safety objectives**

- The company's management has to ensure that safety objectives and safety performance targets are established for all functional areas and levels of the company that may have an influence on safety. This also includes the safety objectives and safety performance targets for process execution and process results.
- The safety objectives have to be measurable and in accord with the safety policy. By establishing safety objectives, the safety policy is converted into operating instructions for safety-relevant processes/activities (e. g. operation of the plant, maintenance and repair, experience feedback, human resources management, etc.).

- A procedure specifying how changes in the safety policy influence safety objectives has to be established.

### **3.2.5 Management by setting examples**

- The managers of the company have to identify with and actively support the company's safety policy.
- Line managers have to assume an exemplary and controlling function. This includes
  - the monitoring of processes within their area of responsibility and the checking of process results,
  - being present at the workplaces (safety inspection rounds, regularly recurring inspections at workplaces with safety relevance, talking to employees on the shop floor),
  - correcting bad safety practices, and
  - promoting and setting examples of good safety practices and being committed to continual improvement.

### **3.2.6 Definition of the organisational structure**

- Top management has to ensure that an organisational structure is defined that is expedient with regard to safety and that tasks, responsibilities and authorities (authority to make decisions and give instructions) within the company right down to the execution level are allocated, agreed with those concerned, and communicated. Here, the requirements ensuing from the German nuclear laws and regulations have to be taken into account. Examples are tasks, responsibilities and competences as well as their organisational association that result from the Radiological Protection Ordinance /1/ and the Nuclear Safety Officer and Reporting Ordinance /11/.
- The position, tasks, responsibilities and authorities of managers have to be specified clearly. Here, the agreement of task, authority and responsibility has to be observed (principle of compatibility). The allocation of tasks to managers has to be thus that there will be no conflicting interests for individuals.

- The tasks, responsibilities and authorities of superior organisational units of the company and of the plant's organisational unit, of the different organisational units within the plant as well as of external organisations (e. g. vendors, suppliers) have to be clearly defined and delimited from each other without any overlap.
- It has to be ensured that control and responsibility for all safety-relevant processes is assigned to the plant's top management and organisational units in charge. It furthermore has to be ensured that the individuals concerned have the necessary competence from a technical and organisational point of view to assume responsibility for safe operation.
- The organisational structure and the associated specifications have to be documented. This includes i. a. an organisation chart and job descriptions for all jobs/groups of jobs within the organisation.
- The organisational structure with the associated specifications has to be checked regularly for its adequacy to ensure safety. If necessary, it has to be revised.

### **3.2.7 Communication**

- Top management has to ensure that appropriate communication processes are established within the company. The communication systems have to be kept in good working condition and their use has to be promoted. Depending on the relevance of the information, communication may be formal or informal.
- The communication system has to systematise the communication channel top-down as well as bottom-up and has to contain the following aspects:
  - communication of the safety policy so that everybody within the company understands this policy and is aware of his/her role in ensuring safety,
  - communication of the company's safety objectives and the derived detailed safety objectives for process execution and process results,
  - communication of the organisational specifications,
  - imparting of knowledge regarding legal and official requirements and of the plant's safety specification, all rules governing the execution of safety-relevant activities as well as of all new findings in the field of safety,

- systematisation of the exchange of information between managers and their staff, between working groups, and between different shifts,
  - transmission of the information necessary for the execution of safety-relevant activities,
  - encouragement of the personnel to give feedback on safety concerns.
- Top management has to ensure that communication takes place with external organisations (e. g. suppliers, regulatory authorities, experts, other nuclear power plants, operating organisations) via well-defined and effective communication channels.

### **3.2.8 Top management review of the safety management system**

- The top management has to review the company's safety management system at regular planned intervals on the basis of the external and internal requirements to ensure its continuing suitability, adequacy and effectiveness. This review has to include assessing opportunities for improvement of the safety management system and the need for changes to the safety management system, including the safety policy and the safety objectives.
- The management review has to take the following information into account:
  - results of audits,
  - results of the measuring of process performance (process execution and process results),
  - status of corrective actions and improvement measures,
  - status and results of the measures following up previous management reviews,
  - feedback from external organisations (authorities, experts, contractors, etc.)
  - changes with an effect on safety management (technical, organisational-administrative changes such as modifications of internal and external requirements).
- Decisions have to be derived from the management review with respect to the need for improvement of the safety management system and safety performance as well as with regard to the necessary resources.

### **3.3 Management of the necessary resources**

#### **3.3.1 Provision of resources**

- The company has to determine, provide and maintain on the basis of a comprehensible procedure the resources that are necessary for implementing the safety policy meeting the safety objectives. These comprise
  - a plant that can be operated safely,
  - the necessary tools, equipment and machinery,
  - qualified personnel (including contract personnel and suppliers) in sufficient numbers,
  - an adequate work environment,
  - the resources needed for the implementation, maintenance and continual improvement of safety management.

#### **3.3.2 Human resources**

- The company has to determine, provide and maintain sufficient numbers of qualified personnel required in the following areas to perform safety-relevant activities and to maintain core competences:
  - plant operation
  - maintenance (mechanical engineering, instrumentation and control)
  - monitoring (e. g. radiation protection, chemistry, physical protection)
  - technical support (e. g. feedback of experience, preservation of technical qualification, modification of technical systems or in the area of organisation/ administration, technical analyses)
- Personnel qualification and capacity has to be thus that the requirements resulting from the safety policy and the safety objectives can be fulfilled. Here, personnel qualification and capacity resulting from the safety-related requirements for deputy and on-call regulations also have to be taken into account.

- Personnel qualification and capacity has to be regularly reviewed and, if necessary, adapted.
- The company has to make suitable provisions for the selection, deployment and training of its personnel in order to ensure the necessary technical and personal competence (physical suitability, reliability, willingness to communicate, ability to work in a team) of the employees. Here, the requirements contained in the Guidelines on Technical Qualification /2, 7/ have to be considered in particular. The company has to
  - determine the necessary competence for personnel performing safety-relevant activities,
  - ensure and document that the necessary skills are imparted by providing training for the personnel by means of systematic training programmes,
  - ensure that by regular reviews the knowledge and skills of the personnel are determined and that the competence of the personnel is maintained by suitable refresher courses derived from the reviews.

### **3.3.3 Infrastructure**

- The company has to determine, specify, provide and maintain the infrastructure needed to establish the safety policy and achieve the safety objectives. Infrastructure includes resources such as the plant itself including its process equipment (hard- and software), tools, auxiliary materials as well as supporting services (information, communication, transport).
- The process of determination, specification, provision and maintenance of the infrastructure has to consider:
  - internal and external requirements, especially safety requirements;
  - maintenance measures to ensure that the infrastructure always meets internal and external requirements. The kind and frequency of maintenance and the verification of the functional performance of each infrastructure component depends on its safety relevance;
  - environmental effects associated with the infrastructure;
  - risks involved as a result of external impacts on the infrastructure.

#### **3.3.4 Work environment**

- The company has to determine, provide and maintain the work environment needed to establish the safety policy and enable the employee to achieve the safety objectives. The work environment has to
  - positively influence the employee's motivation, satisfaction and performance,
  - allow the work to be performed in a safe manner without any unreasonable physical and mental strain on the employees.

#### **3.3.5 External organisations**

- Co-operation with external organisations (authorities, experts, vendors, suppliers, contractors) has to be arranged and co-ordinated. The interfaces with external organisations have to be defined.
- Obligations to authorities and experts within the framework of official procedures have to be determined and considered in the planning and performance of work.
- The tasks and responsibilities of the other external organisations have to be defined.
- It has to be ensured that the general control and responsibility of safety-relevant activities rests with the plant director and therefore with the plant's organisational units in charge. The number of personnel needed for the specification and acceptance of work and for the supervision of contractors and auxiliary personnel by the licensee's own personnel has to be determined and defined. The licensee's personnel has to be specially qualified and trained to fulfil these functions. In addition, sufficient time and personnel has to be provided for these tasks.

#### **3.3.6 Specialist competence in key areas**

- It has to be ensured for key areas where high safety has to be guaranteed that the necessary specialist competences are maintained in the long run, both externally and internally. This includes the adaptation of the necessary specialist competences to the state of the art in science and technology.
- Rules have to be provided for

- the suitable determination and monitoring of the existence of the necessary specialist competences (external and internal),
- reactions to competence loss.

### **3.4 Work realisation**

#### **3.4.1 Planning of work realisation**

- The company has to plan and develop the processes necessary for performing the safety-relevant activities quality-assured with the aim to guarantee safe and effective performance. This also has to include those processes that are necessary to control anomalies, incidents and emergencies.
- In planning the processes, the following has to be determined:
  - Safety objectives and requirements for process execution and process results. Here, the requirements for the processes of other management systems have to be included. Any incongruous requirements have to be harmonized. It has to be ensured that the requirements that have to be fulfilled to guarantee safety have priority.
  - Precautionary measures to avoid mistakes and to prevent the effects of any mistakes that have been made.
  - Required verification, validation, monitoring and inspection stages, with the associated criteria for the review of the processes and process results.
  - Records needed to provide evidence that the processes and process results fulfil the requirements.
  - Required activities, measures and resources for reaching the desired process result.
  - Safety measures that have to be provided to avoid health and safety risks during the performance of the work. Risk assessments have to be used in determining these safety measures. The degree of detail of the risk assessment shall depend on the level of the respective risk.

### **3.4.2 Determination of the requirements for process execution and process results**

- Requirements have to be determined for each process that have to be made from a safety-related point of view with regard to process execution and the process results. These are on the one hand external requirements, such as legal and official requirements, or requirements resulting from expectations by e. g. the general public. On the other hand, they are internal requirements ensuing from the company's safety policy and safety objectives.
- The requirements for process execution and the process results have to be reviewed. This review has to be made before any new or modified requirements enter into force and has to ensure that the requirements
  - are clearly defined and
  - can actually be fulfilled.
- The requirements for process execution and process results have to be defined and documented. If requirements change, it has to be ensured that the associated documents are also amended and that the personnel in charge is adequately informed.
- Upon defining the requirements for process execution and process results, care has to be taken that external and internal requirements are in agreement with each other. In this respect, the company has to define and establish rules for effective communication, especially with supervisory authorities and experts as well as with the general public, in order to impart the company's own safety requirements and determine external requirements as soon as possible.

### **3.4.3 Design and development**

Design and development may include new designs or development work in connection with modification projects. Both are referred to in the following as "design and development". Design and development may concern all areas, such as technical systems, procedures, methods or organisational/administrative measures and rules (e. g. organisational structure, processes, instructions).

- Design and development has to be planned, controlled and documented. This includes
  - the determination of the design and development stages, including the implementation phase and the implementation plan,
  - the ensurance of adequate review, verification and validation for each design and development stage,
  - the determination of the responsibilities, tasks and authorities of the individuals and groups involved in design and development. The interfaces between the individuals and groups involved have to be determined and described. The combined acting of the individuals and groups has to be controlled to ensure effective communication and clear assignment of responsibility.
- The degree of detail and the scope of planning and reviewing a design and development process have to be in line with the safety relevance of the design and development. The design and development process has to be documented.
- The requirements for the outputs of design and development have to be determined and laid down in detail. These requirements have to be reviewed for adequacy. The requirements have to be complete, unambiguous and not in conflict with each other.
- The outputs of design and development have to be provided in a form that allows their review with regard to the requirements. The outputs of design and development have to fulfil the requirements.
- During design and development, reviews have to be performed of whether the design and development is leading in the right direction. For this purpose, design and development stages have to be determined according to which such a review has to be performed. If necessary, countermeasures have to be derived and implemented.
- The outputs of design and development have to be verified in accordance with planned arrangements. Their verification is to ensure that the outputs of design and development fulfil the requirements. The results of the verification and the measures derived have to be documented.
- The outputs of design and development have to be validated (e. g. by commissioning) in accordance with planned arrangements. Their validation is to

ensure that the outputs of design and development fulfil the requirements under the planned conditions of service. The results of the validation and the measures derived have to be documented.

- Especially in the design and development of organisational changes and changes in view of system design it has to be ensured that all necessary safety precautions are maintained in the implementation of the changes. The necessary numbers of trained and competent personnel has to be determined and provided in time, especially for new jobs arising in connection with the changes or for jobs that are attributed wider areas of responsibility. To promote understanding and acceptance of changes, these have to be communicated and, if necessary, planned with involvement of the personnel.
- If requirements change as a result of design and development, these changes have to be identified and documented. The changes have to be reviewed, verified and validated and have to be approved prior to their implementation. This review also has to consider the effects on already existing results of the design and development process. If necessary, parts of the design and development process or the entire design and development process have to be run through once again. The results of the review of the changed requirements and any necessary measures derived have to be documented.

#### **3.4.4 Purchasing**

- The company has to determine and realise a process for effective and efficient purchasing of products (services, auxiliary materials, hard- and software) within the company and from external organisations (suppliers, contractors).
- In this purchasing process, the company has to
  - identify the need for and the specifications of the product to be purchased;
  - ensure by suitable testing and verification that the purchased product complies with the specifications (e. g. qualification test). The kind and scope of the testing and verification of the product depend on its safety significance;
  - take logistic requirements into account;
  - make sure that the product is identified and can be traced back;

- make sure that records are kept.
- The company has to evaluate whether an external organisation is capable of meeting the requirements that exist for the product to be purchased. External organisations have to be evaluated and selected according to specified criteria. Requirements have to be defined for the qualification of the personnel and for the safety and quality management of the external organisation. Upon the selection of vendors, suppliers and contractors, the qualification to fulfil the planned task and aspects of safety have to be considered in particular. The evaluations of external organisations have to be documented.
- Vendors, suppliers and contractors have to be involved in the safety management system. Here, important aspects are an adequate exchange of information, training and instruction, monitoring of skills and evaluation as well as appreciation of successful efforts and achievements regarding safety.
- Contractors have to fulfil the same requirements for safety performance as the company's own personnel.
- The company continually has to evaluate the experience with external organisations with regard to their compliance with safety and quality requirements. In case of any deviations, corresponding action has to be taken.

#### **3.4.5 Materials management**

The company has to maintain the conformity of the purchased product from the moment of purchase until the time when it is internally used. This includes the identification, handling, packaging, storage and protection of the product.

#### **3.4.6 Execution of work**

- The company has to plan and carry out safety-relevant work under controlled conditions. Controlled conditions shall include, as applicable,
  - the availability of internal and external requirements (details on safety objectives as well as on process targets and process results),
  - the availability of work instructions,

- the use of suitable equipment,
  - the availability and use of suitable monitoring and measuring devices,
  - the execution of monitoring and measuring (e. g. in-service inspections) and the approval of process results.
- All safety-relevant processes whose results cannot be verified by subsequent measuring or monitoring have to be validated.
  - Rules have to be laid down for all safety-relevant activities to ensure a status identification of each activity's state of implementation. The aim is to check and coordinate the sequence of activities, to document progress, and to ensure the traceability of the activities (e. g. operational management systems, check lists, etc.).

#### **3.4.7 Control of monitoring and measuring devices within the framework of work realisation**

- The company has to determine for all safety-relevant processes the monitoring measures and measurements and the monitoring and measuring devices needed to provide evidence of the conformity of process execution and process results with the requirements.
- The company has to develop and establish processes to ensure that monitoring and measuring can be carried out and is carried out in a manner that is consistent with monitoring and measuring requirements.
- The qualification of the monitoring and measuring devices has to be ensured (calibration, adjustment, verification and identification of the calibration status, protection against damage).

### **3.5 Measuring, analysis and improvement**

#### **3.5.1 General**

- The company has to plan and implement the monitoring, measuring, analysis and improvement processes needed

- to show that safety objectives have been fulfilled and process results achieved,
- to ensure the effectiveness of the safety management system and the processes,
- to continually improve the effectiveness of the safety management system and the processes.

### **3.5.2 Monitoring of safety performance and processes**

- The company has to develop a suitable objective evaluation system for the routine monitoring and measuring of safety performance and of the effectiveness of the processes with regard to the conformity of process execution and process results with the requirements. This is to ensure that the safety performance targets and the requirements for process execution and process results are fulfilled and safety performance is improved. This system has to provide the possibility to make projections and has to comprise reactive as well as active evaluations. Wherever possible and appropriate, measurable indicators have to be developed and established for monitoring safety performance and processes, especially process execution and the process results.

### **3.5.3 Treatment of inadequate process results**

- The company has to determine a procedure for the treatment of inadequate safety performance and inadequate process results. This includes the determination of measures to
  - eliminate detected deficiencies,
  - rectify deviations from the requirements to ensure conformity of the process execution and process results, and
  - prevent the use of products/process results that do not fulfil the corresponding requirements.
- Any mistakes that have been made have to be evaluated to identify possible trends. Negative tendencies have to be taken into account for improvements (experience feedback) and as input for the management evaluation.

- Mechanisms have to be established for the reporting of safety-relevant observations and findings on the part of the employees; these mechanisms may be formal (e. g. safety meetings, HF system) and informal (e. g. notification of line management).
- The company's top management shall commit and encourage its employees to report any mistakes at any state of a process in order to ensure their timely recognition and rectification.

#### **3.5.4 Internal audits**

- The company has to perform internal audits at regular intervals to determine whether the safety management system fulfils the internal and external requirements (legal/official requirements and requirements laid down by the company itself) and whether it is effectively put into practice and maintained.
- The importance of the processes to be audited is to be considered in the determination of the criteria, scope, frequency and methods of the audits.

#### **3.5.5 External audits**

- The company should have audits and reviews performed by independent organisations to provide judgement on the effectiveness of the safety management systems against external best practices. These audits and reviews include e. g. Peer Reviews carried out by international agencies (e. g. IAEA-OSART, WANO) or local reviews involving staff drawn from other sites within the utility or from other utilities.

#### **3.5.6 Improvements**

- The company has to establish a procedure for the continual improvement of the effectiveness of all elements of the safety management system.
- The company's top management has to establish a culture of promoting the commitment to continual improvement within the company, actively involving the personnel in the development of improvement measures.

- Arrangements have to be made to co-ordinate the various improvement initiatives and identify priorities and resources. Priority improvement measures shall be determined on the basis of safety considerations, taking into account the results of process monitoring, audits, reviews and other relevant information sources.
- The improvement programme routinely has to
  - be monitored against specified objectives,
  - be monitored against its compliance with schedules (including reviews and revisions of schedules as appropriate) and
  - involve senior managers.

### **3.5.7 Corrective actions**

- The company has to take corrective actions to eliminate the causes of any errors so that repeats are avoided. The development and implementation of suitable corrective actions has to be ensured by the monitoring of deadlines and validation of the actions.
- The planning of corrective actions has to be appropriate to the importance of the problems and has to include possible effects on factors such as safety, process performance, process reliability, and operating costs.

## 4 Definitions

These 'Fundamentals' use the following terms with the definitions given below:

### **Activity:**

Production of work results such services, hardware, software, documents, decisions, etc.

### **Company:**

A company whose owner (AG, GmbH, OHG or other form) is the operator of a nuclear power plant and holds the corresponding requisite licence according to § 7 Atomic Energy Act; the company comprises the personnel, equipment and rights, including the organisation, necessary to operate the nuclear power plant. Other companies with a share in the company, dominant companies or companies otherwise associated or parts of such companies that are referred to in the operator's documentation of the safety management system as far as they assume tasks and responsibilities relevant to the safety of the nuclear power plant shall also be considered as part of the company.

### **Development:**

Set of processes transforming requirements into defined features or into the specification of a product, process or system.

### **Management:**

Co-ordinated activities to manage and control a company.

### **Organisation:**

Group of persons and institutions with a structure of responsibilities, authorities and relationships (e. g. company, corporation, firm, enterprise).

In these 'Fundamentals', the term organisation is used on the one hand meaning an institution (institutional aspect) and on the other hand meaning the structure installed to reach the business objectives (instrumental aspect). The respective meaning of the term ensues from the context.

### **Procedure:**

Established way of carrying out an activity or process.

**Process, safety-relevant:**

The safety-relevant processes comprise those processes that have a direct influence on safety, such as the operation of the plant and maintenance, as well as those processes that have an indirect influence on safety, such as management processes and supporting processes.

**Process:**

A process consists of a set of interrelated or interacting activities that converts input into results.

**Process-oriented approach:**

The application of a system of processes within a company reflecting the activities within the company. The systematic recognition and handling of these processes as well as of the interactions between the various processes is referred to as "process-oriented approach".

**Product:**

A product is the result of a process. This may be services/activities, hardware, software/documents, organisational and administrative regulations, etc.

**Safety culture:**

Safety culture is the entirety of all features and behaviours within a company and of individuals which puts beyond doubt the fact that nuclear safety, having overriding priority, receives the attention it is due because of its general importance. Safety culture concerns the organisation as well as the individual.

**Safety management:**

Safety management is the entirety of all activities relating to the planning, organisation, management and control of individuals and working activities with a view to the efficient achievement of a high level of safety performance, i. e. to the achievement of a high quality of all activities that are relevant to safety, and to the promotion of a highly developed safety culture. Safety management is not restricted to specific organisational units but comprises the entire safety-related organisation of the company.

**Safety management system:**

A safety management system comprises all definitions, regulations and organisational aids provided within the company to carry out safely all safety-relevant tasks and to

check and improve target fulfilment. The safety management system represents a tool with which the company promotes and supports a high level of safety culture.

**Safety performance:**

The company's safety performance is the measure of its achievement of safety-relevant objectives.

**Top management of the company:**

Individuals or groups of individuals that manage and control a company at top level.

**Validation:**

Confirmation by provision of objective proof that requirements established for a certain intended use or a certain intended application are fulfilled (e. g. by commissioning test).

**Verification:**

Confirmation by provision of objective proof that requirements are fulfilled.

## 5 References

- /1/ Verordnung über den Schutz vor Schäden durch ionisierende Strahlen (Strahlenschutzverordnung – StrlSchV) vom 20. Juli 2001 (BGBl. I S. 1714, 2002 I S. 1459) geändert, durch Artikel 2 der Verordnung vom 18. Juni 2002 (BGBl. I S. 1869)
- /2/ Richtlinie für den Fachkundenachweis von Kernkraftwerkspersonal, Bek. d. BMU vom 14.04.1993, GMBI. 1993 S. 358
- /3/ IAEA Safety Standards Series, The Operating Organization for Nuclear Power Plants, Safety Guide No NS-G-2.4, Wien, 12/2001
- /4/ INSAG-13, Management of Operational Safety in Nuclear Power Plants, IAEA, Wien, 1999
- /5/ Richtlinie 96/82/EG des Rates vom 9. Dezember 1996 zur Beherrschung der Gefahren bei schweren Unfällen mit gefährlichen Stoffen, ABl. EG 1997 Nr. L 10, S. 13 (Seveso-II-Richtlinie), zuletzt geändert durch Richtlinie 2003/105/EG des Europäischen Parlaments und des Rates vom 16. Dezember 2003 (ABl. EG Nr. L 345 S. 97)
- /6/ Zwölfte Verordnung zur Durchführung des Bundes-Immissionsschutzgesetzes (Störfallverordnung – 12. BImSchV) vom 26. April 2000, Anhang III: Grundsätze für das Sicherheitsmanagementsystem BGBl. I S. 603)
- /7/ Richtlinie über die Gewährleistung der notwendigen Kenntnisse der beim Betrieb von Kernkraftwerken sonst tätigen Personen, Bek. d. BMU vom 30.11.2000, GMBI. 2001 S. 153
- /8/ KTA 1201 „Anforderungen an das Betriebshandbuch“, Fassung Juni 1998, BAnz. 172a vom 15.09.1998
- /9/ KTA 1401 „Anforderungen an die Qualitätssicherung“, Fassung Juni 1996, BAnz. 216a vom 19.11.1996

- /10/ KTA 1404 „Dokumentation beim Bau und Betrieb von Kernkraftwerken“, Fassung Januar 2001, BAnz. 235a vom 15.12.2001
- /11/ Verordnung über den kerntechnischen Sicherheitsbeauftragten und über die Meldung von Störfällen und sonstigen Ereignissen (Atomrechtliche Sicherheitsbeauftragten- and Meldeverordnung – AtSMV), (BGBl. I 1992, 1766), zuletzt geändert durch Artikel 5 der Verordnung vom 18. Juni 2002 (BGBl. I S. 1869)