# QUALITY-SAFETY MANAGEMENT AND PROTECTIVE SYSTEMS FOR SPES

D. Benini, S. Canella, INFN-LNL, Legnaro, Italy

*Abstract*

The realization of a nuclear facility for the production of radioactive ion beams requires a deep study of the safety aspect: an high degree of reliability in the Protective System must be achieved to prevent hazardous situations for operators, population and the surrounding environment.

For the INFN SPES project, a *Quality and Safety Management System* is going to be realized. In this work we will present its general structure, functions and goals. We will then focus our attention on the Access Control and Dose monitoring systems which are the key features of the SPES *Protective System* in the framework of the QSMS.

## INTRODUCTION

SPES (*Selective Production of Exotic Species*) is a INFN project for the realization of a Radioactive Ion Beam facility at Legnaro National Laboratory (LNL).

The radioactive beams production method is based on the ISOL technique (*Isotope Separation On Line*). The exotic isotopes are extracted from proton induced fission products in a UCx direct target, typical expected fission rates are of $10^{13}$ fission/s. The SPES proton driver is a two exit port cyclotron with a variable energy from 15 MeV up to 70 MeV, the foreseen maximum current value is 0,750 mA. A general layout of the SPES facility is illustrated in Fig. 1.

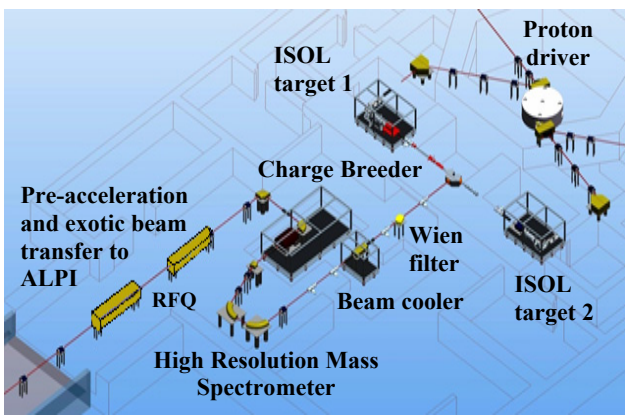


Figure 1: SPES layout.

An overall tool for managing the safety issues of SPES is the Quality and Safety Management System (QSMS), its development is one of our goals in the next future. The implementation of this System starts from the definition of the safety and quality policies to be achieved and involves the drafting of a hierarchical framework of procedures. The Access Control and the Dose Monitoring Systems will be also analyzed for the production of specific documentation.

The Protective System of SPES will be designed with the necessary intent of achieving a high level of safety and reliability, in this way dangerous situations for people and the environment will be avoided. In this paper we present the QSMS concept and its software implementation, the specific features of the SPES Protective System will also be described.

## THE QSMS OF SPES

The QSMS is a managing tool that LNL has chosen to realize for handling all the phases of SPES starting from the initial stage of the facility design.

It is implemented according to Italian laws, technical standards and all mandatory prescriptions that the project must comply. Moreover the international standard ISO 9001:2008 for Quality and OHSAS 18001:2007 for Safety will be the main reference for the development of the QSMS.

An Environmental Management System (ISO 14001:2004 compliant) is already operative at LNL: the QSMS of SPES will be developed considering its structure and also the possible future integration between the two systems.

The first step for the implementation of the System is the definition of a policy of Quality and Safety for SPES, it will be pursued through the definition and the realization of specific objectives. The approach of the QSMS is to divide the SPES project in the following 5 phases of its lifecycle:

- Design;
- Realization;
- Operation;
- Maintenance;
- Disposal.

Every stage will be analysed to identify the activities that should be controlled to guarantee safety and quality for the SPES facility: starting from general guidelines the specific operating instructions for each area will be identified. Some of the aspects that will be analysed for the phases of design and construction concern, for example, the collection of all technical drawings, the identification of legal and technical requirements and the description of the techniques for hazards and risks analysis. Afterwards all the ordinary and emergency procedures for the last three phases (operation, maintenance and disposal) will be drawn.

The complete documentation concerning the QSMS is collected and catalogued according to specific storage rules that allow a fast identification of each document and an easy retrieval in the electronic archive. Documents are hierarchically organized according to a pyramidal scheme: at the top we find the general paper describing the QSMS in its whole, moving downward there are more

precise documents explaining with more details each specific activity.

Figure 2 shows the documents organization scheme of QSMS.

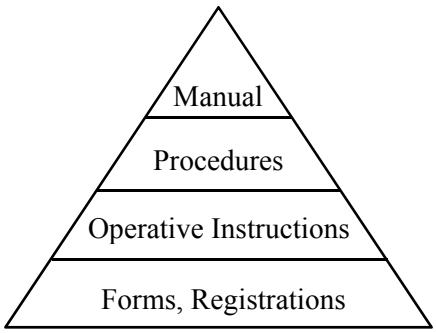


Figure 2: Scheme of the QSMS documentation.

Documents are divided in the following categories:

- Manual: is the text describing the QSMS general features explaining its purposes and organization modalities;
- Procedures: these documents describe how every single activity foreseen by the System has to be performed. They are divided in Managerial and Technical considering their connection to the organization of the management system rather than specific SPES activities;
- Operative instructions: they refer to specific procedures and contain a detailed description of how a specific activity has to be performed;
- Forms and registrations: these are report documents to be filled at the end of each activity. They are intended for operations logging.

### *Procedures for the Risk Analysis and the SPES Protective System*

In this work we want to focus the attention on the procedures of the QSMS related to the Risk Analysis of the plant and the Protective System of SPES.

Concerning the Risk Analysis a detailed identification of the hazards and a consequent evaluation of all the risks is needed to optimize both plant design and safety systems. From the point of view of the necessary documents we are preparing a procedure describing the standard techniques that must be applied, the plant and the specific components that must be analysed, the data reports standards. The investigation method requires the use of the following techniques:

- Failure Mode and Effect Analysis (FMEA): with this method one looks for any possible failure of the plant of interest, finding out its gravity and frequency of occurrence. This is done to underline possible design errors of the plant or the presence of single components loosely reliable.
- HAZard and OPerability analysis (HAZOP): process variables are examined looking at the deviations from standard operative conditions. This is done to evidence possible failing situations of the system which can lead to an accident (called Top Event, TE).
- Fault Tree analysis (FT): it evaluates the frequency of occurrence of the TEs evidenced with the HAZOP method.

The results obtained from the combined use of this three methods give an important input for the design and the realization of the SPES Protective System. The guidelines indicated by the LNL's radiation protection officer will be another reference point to take into account, this kind of requirements will have to be completely fulfilled.

From the point of view of the QSMS the documents for the SPES Protective System will contain a detailed description of the safety disposals organization and the single procedures (ordinary and of emergency) to be followed during the facility operation.

## THE SOFTWARE OF THE QSMS

The management of the data flow foreseen by the SPES QSMS will be realized through a custom software. This tool is designed to facilitate the application of the procedures of the QSMS during the different phases of the facility lifecycle. It will have to act as data collector during the project realization as well as an automation tool for the working and maintenance procedures.

We intend to realize a user-friendly interface enabling every-day use, easy procedures retrieval and fast actions logging. Flexibility is also one of the most important features, for this reason a modular structure will be implemented so that each unit can be developed, created or cancelled as needed.

### *Technical Description*

From the technical point of view, the software is composed of two parts:

- a Relational Database Management System (RDBMS) for data collection;
- an interface that allows users interaction with the data stored in the database. To allow easy distribution of the software and multi-platform support, a web-based application has to be preferred.

To realize this project a dedicated website will be realized on proper LNL servers using the standard Apache/PHP/MySQL open source platforms.

The database is going to be divided in the following main units:

- SPES elements* of these four main areas: experimental plant, laboratories, safety systems, infrastructures (buildings, plant);
- Personnel;
- Documents;
- Stocks;
- Suppliers and other contacts;
- Laws and technical standards;

* Elements are all the equipment, plant and infrastructures in which the project SPES can be subdivided.

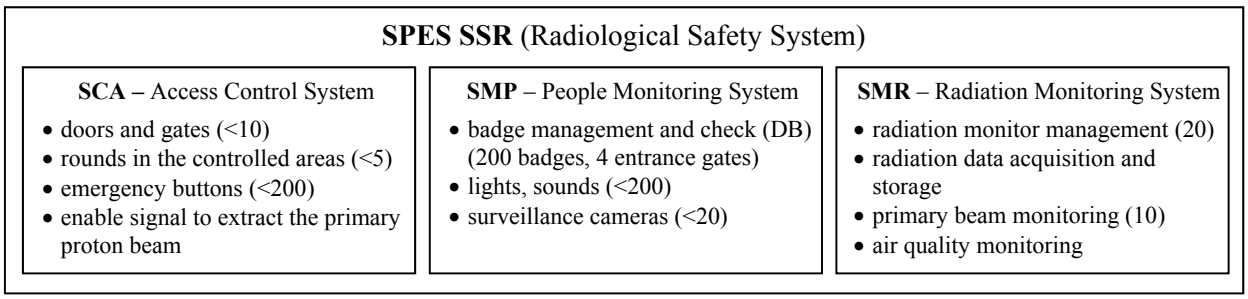


Figure 3: The three elements of SSR with the foreseen number of objects to be managed.

- Procedures (operation of equipment, maintenance, emergencies, accidents, etc.);
- Audit.

In the framework of the QSMS we will develop the SPES Protective System illustrated in the following paragraph.

## THE SPES PROTECTIVE SYSTEM

The SPES Protective System will be an instrumented system with the function to detect potentially dangerous conditions for people and the environment, when such a state is detected it will have to execute a sequence of actions to restore a safe state.

For this goal, the SPES protective system will be characterized by the following attributes:

- independence from the process managing the plant, that is from the SPES control system;
- its integrity and functionality has to be maintainable and always be verifiable;
- high reliability (redundancy, at least in the most critical parts for safety);
- any access to it (for checks or maintenance) is to be performed under surveillance and monitored;
- changes are always to be logged, approved and promptly documented.

These attributes have to be maintained by good administration practices (i.e. by QSMS).

### *The Structure of the Protective System*

The structure of SPES Protective System will rely on two interconnected sub-systems: one for conventional, the other for radiological risks. During the operating periods, a Conventional Safety System (**SSC** - Sistema di Sicurezza Convenzionale) will avoid/reduce the risks related to standard engineering (high voltage, water cooling, venting systems). The Radiological Safety System (**SSR** – Sistema di Sicurezza Radiologica) will avoid/reduce the following risks:

- irradiation and contamination of people both when SPES is running and when it is off (activated materials may still be present in the plant site);
- any case of uncontrolled sprinkling of radioactive material outside the SPES complex.

Both the SSC and SSR must avoid/reduce the safety risks also when SPES control systems and the protective systems themselves are off or in fault: they must be fail-safe.

With more details, SSR will be made up by three elements:

- an Access Control System (Sistema Controllo Accessi – **SCA**) for gates and doors, for rounds in the controlled areas, for emergency buttons and for the final enabling control signal to the primary proton driver;
- a People Monitoring System (Sistema di Monitoraggio delle Persone – **SMP**), to enable/disable people access to different building areas (by badges/tokens), to manage warning lights and tables, sounds, surveillance cameras;
- a Radiation Monitoring System (Sistema di Monitoraggio delle Radiazioni – **SMR**), to control radiation monitors, to acquire and store related data, to manage thresholds and produce alarms and interlocks, to monitor the primary proton beam quality, to check the activation level of pumped air to be eventually released outside the SPES complex.

Figure 3 shows a scheme of the SSR with its elements.

The whole SCA system will be redundant at least at level 2: two parallel systems will acquire the same signals and produce the final enable/disable output for the primary beam accelerator. In particular, a first system will be based on safety-oriented PLC architecture, while a second one, minimal but highly reliable, will be made of embedded ("custom") not-programmable logic cards (for example with FPGA based logic modules).

The SCA system will have to produce the enabling signal for the proton beam extraction from the cyclotron. Its high reliability will be based on redundancy and high quality of the hardware system for the IN/OUT signals from the field (gate and door status, round and emergency buttons) and to the actuators which will be produced by redundant detectors and command chains (at least 2 for each gate and door and for the main beam shutters), separately cabled.

For the SMP section and SMR (radiation monitors), a highly reliable PLC based architecture should be sufficient.

Any fault or anomalous behavior in any of these sub-systems will have as direct consequence the switching off of the primary beam.