Quality Assurance applied to Accelerator Safety

Magali Gruwé and Ghislain Roy
BE-ASR-SU

IEFC Workshop – 11th February 2010

Outline

- Reminder: What is Quality Assurance?
- Examples:
  - Quality Assurance for an equipment (EIS) → **Concept of Safety File**
  - Quality Assurance for a process → **DIMR**
- Conclusion: Some key messages

Reminder: what is Quality Assurance?

- **Quality**:

  Ability for a system or a product to satisfy expected characteristics

- **Quality Assurance**:

  The aim of Quality Assurance is to provide all **stakeholders** with the possibility to acquire the **confidence** that a given process or product meets a set of expected characteristics.

- Key word is **confidence**!

  As a person responsible for an equipment, how can I give you, and other stakeholders, the confidence that my equipment meets the expected characteristics?

Quality Assurance applied to Accelerator Safety

Quality Assurance applied to Accelerator Safety requires the prior identification of :

- The products and processes where it is required
- The Safety Stakeholders and their respective roles
- The expected Safety Characteristics

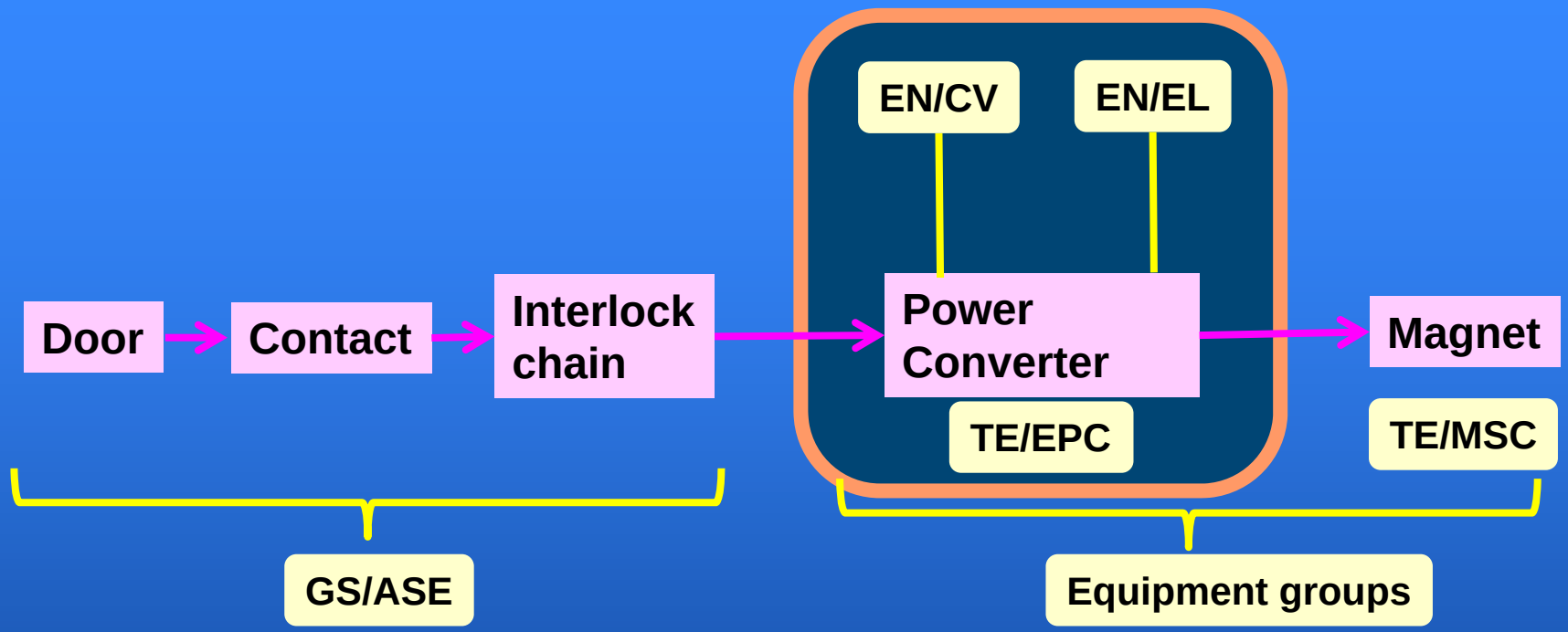
Stakeholders

- **“Users”, workers, personnel**:
  - those who access the areas where they can be exposed to danger
- **Public and local population**
  - those who are on and around the CERN site
- **Management**
  - those responsible in case of “problem”
  - those responsible for the personnel they send to work
- **Safety Commission and Safety Officers**
  - those checking that Safety is ensured
- **Persons** in charge of / **responsible** for the concerned system or equipment:
  - those who know best the system or equipment concerned
- **People who perform interventions** on the system or equipment
- **Control Room Operators**

Outline

- Reminder: What is Quality Assurance?
- Examples:
  - Quality Assurance for an equipment (EIS) → **Concept of Safety File**
  - Quality Assurance for a process → **DIMR**
- Conclusion: Some key messages

Example:
“Élément Important pour la Sécurité”



Example: Power Converter (I)

- What are the **expected characteristics** of the Power Converter **in matters of Safety**?
  - The Power Converter:
    - Should stop when required
      - i.e., to stop beam in case people intrude in the machine
    - Should not start untimely
      - i.e., impossible to put beam when people may be in the machine
    - …
  - These functions should be ensured with minimal impact on:
    - Reliability
      (the ability of a system or component to perform its required functions under stated conditions for a specified period of time)
    - Availability
      (availability is the proportion of time a system is in a functioning condition)

Description

Example: Power Converter (II)

- **Identification of the different processes** :
  - Installation
  - Maintenance
  - Replacement by a spare
  - Test
  - etc…

Description

- **Analysis of each process**, i.e. what could go wrong and what would the consequences be?

  Example for maintenance process:
  - Cable not or badly reconnected
  - By-pass or strap remained in place
  - Power Converter remained in “Local”
  - Wrong software or configuration
  - etc…

Risk analysis

Example: Power Converter (III)

- **What do we do to minimize the risk**, i.e.
  - The probability of occurrence?
  - The consequences?

Risk Management

  - Examples:
    - Fail-safe design
    - Additional strand (if cable is disconnected, an alarm is issued)
    - Well defined procedure

Operating procedures

    - Check-list to be filled at the end of the intervention
    - Second layer of control

Follow-up documents

Safety File

- A **tool**
- A **reference** for an installation / system / equipment containing all data needed to assess its safety compliance
- Formalizes / centralizes / organizes what is often already done, if only partially
- **DYNAMIC** and includes “lessons learnt” (“Retour d’Expérience”)

- A Safety File should contain **5 parts**:
  1. Descriptive part
  2. Risk analysis
  3. Risk Management
  4. Standard Operating Procedures and applicable rules
  5. Operation follow-up documents

Safety File: Descriptive part

- **Description** (of the system or the installation):
  - Questions to be addressed:
    - What are the expected characteristics of the equipment?
    - What are the activities / processes?
    - What could go wrong? What may happen?
  - Content:
    - Description of the equipment / installation
    - Description of the environment
    - Description of the interfaces with and dependencies on other systems
    - A list of dangers

Safety File: Risk analysis

Risk analysis:

- Questions to be addressed:
  - For each possible incident: what are the consequences?
  - How frequently each possible incident might occur?

- Risk evaluation matrix takes into account:
  - Probability of occurrence
  - Severity of consequences

- Risk is the “product” of the probability times the severity

Probabilité d'occurence \ Sévérité des conséquences	CATASTROPHIQUE	CRITIQUE	MARGINAL	NEGLIGEABLE
FRÉQUENT	ÉLEVÉ	ÉLEVÉ	SÉRIEUX	MODÉRÉ
PROBABLE	ÉLEVÉ	SÉRIEUX	MODÉRÉ	FAIBLE
POSSIBLE	SÉRIEUX	MODÉRÉ	MODÉRÉ	FAIBLE
IMPROBABLE	MODÉRÉ	FAIBLE	FAIBLE	FAIBLE

Safety File: Risk Management

- **Risk Management**:
  - Questions to be addressed:
    - What can we do to minimize the probability of an incident?
    - What can we do to minimize the consequences of an incident?
    - What can we do to minimize the risk?
    - What do we choose to do, and why ?
  - Content:
    - Explanation of the technical and organizational choices
  - Purpose is to ensure
    - Adequacy of the system with the requirements
    - Traceability of the technical and organizational choices
    - Validity in time of these choices
    - Coherence (in time) between the system and the safety requirements

Safety File: Standard Operating Procedures and applicable rules

- **SOP and applicable rules**:
  - Questions to be addressed:
    - How do we perform the processes?
    - What are the instructions given to intervening teams?
  - Content:
    - Information notes
    - Instructions and procedures
    - Training
  - Update on regular basis, taking into account the lessons learnt
  - Important : check the adequacy of the instructions and procedures
    - Are they applied?
    - Are they practical?

Safety File: Operation follow-up documents

- **Operation follow-up documents**:
  - Questions to be addressed:
    - How do we have or give confidence that expected characteristics are met?
  - Content:
    - Minutes of meetings
    - Results of tests
    - Check-lists
    - Reports of non-conformities
    - Lessons learnt

Outline

- Reminder: What is Quality Assurance?
- Examples:
  - Quality Assurance for an equipment (EIS) → **Concept of Safety File**
  - Quality Assurance for a process → **DIMR**
- Conclusion: Some key messages

Example: intervention on an equipment

- Intervention on an equipment, e.g. for maintenance :

In case the equipment is radioactive or intervention is to be done in a radioactive environment:

- The **expected characteristics** to be met are:
  Equipment performs as expected after the intervention
  and **Dose is As Low As Reasonably Achievable** (ALARA)

- The intervention procedure should thus include this additional aspect:
  Dose evaluation and planning to respect the “ALARA principle”

Example: intervention on an equipment

- Approach:
  - Description of the work to be performed
  - Assessment of the dose
  - Thoughts about alternatives:
    - Collective work!
    - Thus work and thoughts should be presented and discussed
  - Arguments to show the dose has been minimized
  - Instructions for the intervening team
  - Activity itself
  - Activity report specifying the dose indeed received

Description

Risk Analysis

Risk Management

Operation

Follow-up

Quality Assurance in the context of an intervention procedure

DIMR

- **DIMR**, “Dossier d’Intervention en Milieu Radioactif”:
  - A tool
  - Gives the framework for interventions in radioactive environments
  - Provides:
    - Classification depending on
      - Dose rate
      - Expected personal dose
      - Expected collective dose
      - Radioactive contamination
      - Nature of the intervention (unique or repetitive)
    - Information and decision processes, based on the risk level (**DIMR level I, II or III, depending on risk**)
    - Safety (technical and organizational) measures
    - Follow-up forms, to present and record information about the intervention for future reference
  - DIMR is now being put in place (already used for some interventions)

Key messages

- Quality Assurance:
  - Is NOT meant to stop people from working
  - Is intended to bring confidence amongst all stakeholders
- Do only as much Quality Assurance as required to acquire this confidence :
  - Depending on risk analysis
  - And no point in overdoing it
- One person amongst stakeholders should be responsible for the Safety File of each installation / system, including making sure it is up to date.

  Mandate to be properly defined and names to be identified (BFSP)
- Safety Unit is there to help… but not to do the work for you…