White Paper 2017-01

The ROOTS® method – an innovative reference method for the nuclear safety case development for laboratories, nuclear plants and nuclear decommissioning

The ROOTS® nuclear safety analysis method is a proven, innovative method that combines both a deductive and an inductive risk assessment conducted at the functional level.

The method allows to generate a comprehensive analysis of the facility and responds to the latest requirements for safety cases for nuclear facilities in France. It allows to identify those Elements Important for Safety and Activities Important for Safety and define the related requirements. This leads to operational requirements that are more finely adapted to the safety requirements. The method has the benefits to identify those requirements based on the operational condition of the facility thus providing a much needed flexibility, in particular during decommissioning activities.

The method has been developed by CleanuC and is today proven and implemented in various stages of detail on 5 nuclear facilities in France. Additional implementations are ongoing.

This White Paper describes the method, its justification and the benefits provided in terms of safety case implementation and safety requirements flexibility in nuclear facilities.

The ROOTS® method's principles

A combination of inductive and deductive methods

The power of the method is based on the implementation of both a deductive and inductive analysis. Appendix 1 describes the difference between those methods that are traditionally used in risk assessments, and what their limits are. Their combination as a loop within the ROOTS® method allows to overcome the limitations while taking benefit of their advantages and power.

The ROOTS® method is includes first a deductive analysis based on Unwanted Events (UE) that correspond to excursions outside of the normal operating domain as defined in the safety case. This deductive analysis identifies Triggering Events (TE) at the functional level that correspond to the possible causes of the UE identified. To guarantee an exhaustive approach, CleanuC uses proprietary lists of potential TE based on typical situations in nuclear facilities. These TE cover both technical and human events.

In a second phase an inductive approach is implemented to determine the possible consequences of the Triggering Events (TE) on the facility. This allows to identify Feared Events (FE). The criticality of those Feared Events is measured on the basis of the probability class of the TE and the consequences with respect to the protected interests (employees, public and environment). This consequence is established taking into account available mitigation factors, plus an additional unique, most penalizing failure for the particular scenario.

Finally, so as check the absence of cliff effects, some scenarios resulting from very low probability events or from multiple failure modes, called Cumulative Situations (CS) are added to the analysis.

A method implemented at the functional level

An important element of the method is the functional level approach. This approach allows to aim at exhaustiveness during the inductive phase, and to choose upfront what the level of detail aimed for is when applying the method. Depending on the needs, the method allows to dig shallower of deeper into the detail of equipment and components of the facility or laboratory. This enables a proper adaptation to the objectives sought.

How the multiple identified scenario are managed

After having analyzed the multiple scenario from the inductive phase, to facilitate later phases a more limited number of representative envelope scenario are screened out. Still the method enables to keep the information about criticality (probability / consequence) of all identified scenario. In a future development this will allow to develop a finer probabilistic approach.

The probability / consequence couple of these scenarios is then compared to the safety objectives of the facility. If it is found that the envelope scenario do not fit the pre-set objectives, certain hypothesis on the robustness of certain lines of defense must be revisited and the model re-run until the resilience of the design fits with the expected safety level.

Linkage to the nuclear safety classification of Equipment and Activities

The Activities Important for Safety (AIS) and Equipment Important for Safety (EIS) must be clearly identified and justified as part of the safety case. Related Defined Requirements (DR) are defined. A testing and maintenance program is then defined to guarantee their performance with regard to the DR.

The list of EIS and AIS is deducted automatically from the previously developed analysis, including the consequences inducted by their failure modes.

Proven advantages of the ROOTS® method

Already applied on multiple nuclear facilities in France, the advantages of the method are multiple:

- Provide a structured safety analysis that provides a sound foundation to the safety case, which is not always the way it has been developed historically. This often leads to revisit deeply the list of EIS and AIS, identifying equipment or activities not previously listed and justifying the de-listing of some others,
- The semi-automation of the method allows multiple updates in case of any change to the facility or of its operating conditions. This is particularly useful in the definition stage of a new facility or in the case of facilities in the process of decommissioning,
- Allow an adaptation of the nuclear safety requirements to the actual operating state of the facility. Still guaranteeing the adequate safety level, this allows an increased operational flexibility that generates substantial direct and indirect savings,
- Allow to justify explicitly the list of AIS and EIS, which leads to rationalizing them. In a specific case for example it has allows to remove from the list of EIS the central radiation monitoring system while guaranteeing a better safety level, by pushing the radiation monitoring-related safety functions to an AIS. This has allowed a more robust surveillance and economic gains related to the removal of operational constraints not justified by nuclear safety.

Conclusion

With the ROOTS® nuclear safety analysis method, CleanuC provides a mature and proven method that is fully consistent with the latest regulatory requirements. The ROOTS® method allows apprehending with the required flexibility the various operating states of nuclear facilities such as laboratories, processing facilities and facilities undergoing decommissioning and dismantling works.

The ROOTS® method has the potential to become the reference method in terms of nuclear safety analysis moving forward.

Glossary

AIS	Activity Important for Safety
CS	Cumulative Situation: worst additional failure in addition to a TE
DR	Defined Requirements of EIS and AIS
EIS	Equipment Important for Safety
FE	Feared event
TE	Triggering event
UE	Unwanted event

Appendix 1: deductive and inductive methods for risk analysis

In terms of risk analysis, the methods used are generally categorized between inductive and deductive methods.

The deductive methods start from an Unwanted Event (UE) and aim at identifying what are will possible Triggering Events (TE) and their combinations. A typical example of a deductive method is the Fault Tree analysis. These methods are difficult to use and generally less frequently used compared to inductive methods.

Inductive methods on the other side are simpler. They start from a functional analysis identifying the different components of the system and their possible failure modes (Triggering Event). The consequences of each TE is then inducted. Those consequences can then be rated in terms of criticality to identify the most critical TE. The most well-known inductive methods include FMECA (failure modes and effects criticality analysis), HAZOP, HAZID and a large number of methods used for the prevention of conventional occupational safety risks.

Advantages and drawbacks of those methods are summarized in the following table:

	Deductive	**Inductive**
Advantage	• Allows to consider combinations of failure and common cause failures	• Relatively easy to implement • Exhaustive if conducted at the functional level
Drawback	• Difficult and long to implement • Limited to the Unwanted Event under consideration. • Requires reliability data • Does not guarantee exhaustiveness	• Does not allow to consider failure combinations or multiple failures.