HAL
open science

The double control and its consistency with the double contingency principle

G. Kyriazidi, P. Rippert

▶ To cite this version:

G. Kyriazidi, P. Rippert. The double control and its consistency with the double contingency principle. ICNC 2019 - 11th International conference on Nuclear Criticality Safety, Sep 2019, PARIS, France. cea-02614128

HAL Id: cea-02614128
https://cea.hal.science/cea-02614128v1

Submitted on 20 May 2020

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

THE DOUBLE CONTROL AND ITS CONSISTENCY WITH THE DOUBLE CONTINGENCY PRINCIPLE

G. KYRIAZIDIS[(1)] **- P. RIPPERT**[(2)]
Commissariat à l'Énergie Atomique et aux Énergies Alternatives

[(1)] *DEN – Service d'assistance en sûreté-sécurité (SA2S)*
CEA/Cadarache, F-13108 Saint-Paul-les-Durance, France

[(2)] *DEN – Service d'exploitation et de traitements des combustibles (SETC)*
CEA, Cadarache, F-13108 Saint-Paul-les-Durance, France

* *Corresponding author email:* georges.kyriazidis@cea.fr

ABSTRACT

The double contingency principle is implemented in French nuclear research and development facilities. Regarding nuclear criticality safety in the CEA's Cadarache centre, the double control principle was initiated in the LECA-STAR facility in the early 2000's and generalized to the other (approx. 20) nuclear installations since then.
This paper presents the operational experience gathered from the beginning until now. Some simple statistics are used to illustrate the reliability of the double control principle as applied in the CEA/Cadarache facilities. The significant events registered at the ASN (Autorité de Sûreté Nucléaire – Nuclear Safety Authority) are analysed to demonstrate that defence in depth prevails and the failures that have occurred were detected and corrected by appropriate measures.

KEY WORDS

Double contingency principle, control, hot lab

1. INTRODUCTION

The double contingency principle (DCP) is nowadays very broadly known and quoted in international standards, guides and/or legislations.
In France, the ASN "criticality safety decision" (now part of the French law), defines the DCP as a minimum condition to prevent a criticality accident.
In order to respect the DCP in its facilities, the CEA / Cadarache has set up an organization as well as operating instructions regarding criticality safety.

2. GENESIS OF THE DOUBLE CONTINGENCY PRINCIPLE

In the U.S. D.O.E. Nuclear Criticality Safety Program [1] internet site section "Training/Resources/Heritage videos" one can find C. M. Hopper interviewing the pioneers in criticality safety. In particular, in the "Heritage Video Conference 2000 Excerpt: The Double Contingency Principle", J. T. Thomas explains that DCP is made especially for events that directly influence the system's reactivity of the material you are trying to control and H. Paxton says (author's transcription) "… *I think it was very unfortunate that we even put DCP into the guides to start with back in the early days simply because, it's something that ….a concept…, was used some place in Oak Ridge and we adopted their terms…*".
Today almost all guides [2], [3], [4], contain the DCP principle, but the terms in which this principle is expressed are variable. We find the words **should** [2] or **shall** [3] or **required** [4]. For example a process analysis is a prerequisite for the application of the DCP.

3. FRENCH LEGISLATION AND THE DOUBLE CONTINGENCY PRINCIPLE

From 1984 until 2014 the DCP was part of RFS I.3.c. [5] which is a recommendation. Formally, the DCP was introduced in the French law in December 2014 [6]. The exact terms are:

Article 2-3

Under the cautious design approach provided for in Article 3-1-II of the abovementioned 7 February 2012 decision, the licensee ***shall****, subject to the provisions of Article 2.4 below, apply the following principle:*

- *a criticality accident must under no circumstances occur from a single anomaly;*
- *if a criticality accident can occur from the concomitant appearance of two anomalies, then it is shown that :*
    - *the two anomalies are independent;*
    - *the probability of occurrence of each of the two anomalies is sufficiently low;*
    - *each anomaly is highlighted with the help of appropriate and reliable means, allowing the repair or the introduction of compensatory measures in a timely manner.*

Article 2-4

In the case when he has justified that the principle stated in article 2-3 cannot be applied, the operator ***shall*** *implement technical and organizational provisions which, in compliance with this Decision, render the accident scenarios in question extremely unlikely with a high degree of confidence.*

These three criteria (independence, sufficiently low occurrence and detection of an anomaly within an adequate time) constitute the basis of the "French" DCP for nuclear criticality.
The draft of ASN guide [7] defines the ways of technical or organizational provisions to ensure the sufficiency of the robustness of the DCP by giving the priority to the first of the three following categories:

- passive provisions, i.e. provisions that are not based on active systems or on human interventions;
- active provisions, that is to say provisions based on active systems (servo controls, automation, etc.);
- organizational and human dispositions, i.e. provisions based on human interventions (action of one or more operators, possibly through an active system, etc.).

4. DECLINATION OF THE DCP AT CEA / CADARACHE THROUGH DOUBLE CONTROL

a. Introduction

A few months before the Tokaï Mura criticality accident CEA authorities were giving some thinking about a new criticality safety organization, pending the fact that the CEA/IPSN was on the process to become the independent TSO IRSN. The Tokaï Mura accident made the project to pick up pace and late 2001 a renewed criticality safety organization was set up. This organization was thorough described in [8], [9], and [10], and less detailed in [11] and [12].
By the end of 2001 a Human and Organisational Factors analysis regarding criticality relevant operations was conducted in the INB 55/LECA-STAR[1] facility. The analysis stressed out the point that even though the controls were done normally their documentation did not necessarily permit to know easily if their execution was really done. In other terms, there was a need to strengthen the formal part of the criticality controls and it was the opportunity to perform an "update" of the criticality safety internal organization in particular by strictly applying the DCP when needed.
The analysis was later transformed to a number of procedures, operating rules etc. An organizational note summarizes the structure of the criticality safety documents, as shown on Figure.I.

[1] In France nuclear facilities named Installations Nucléaires de Base (INB) are listed by their number. The exact list can be found in https://www.asn.fr/.

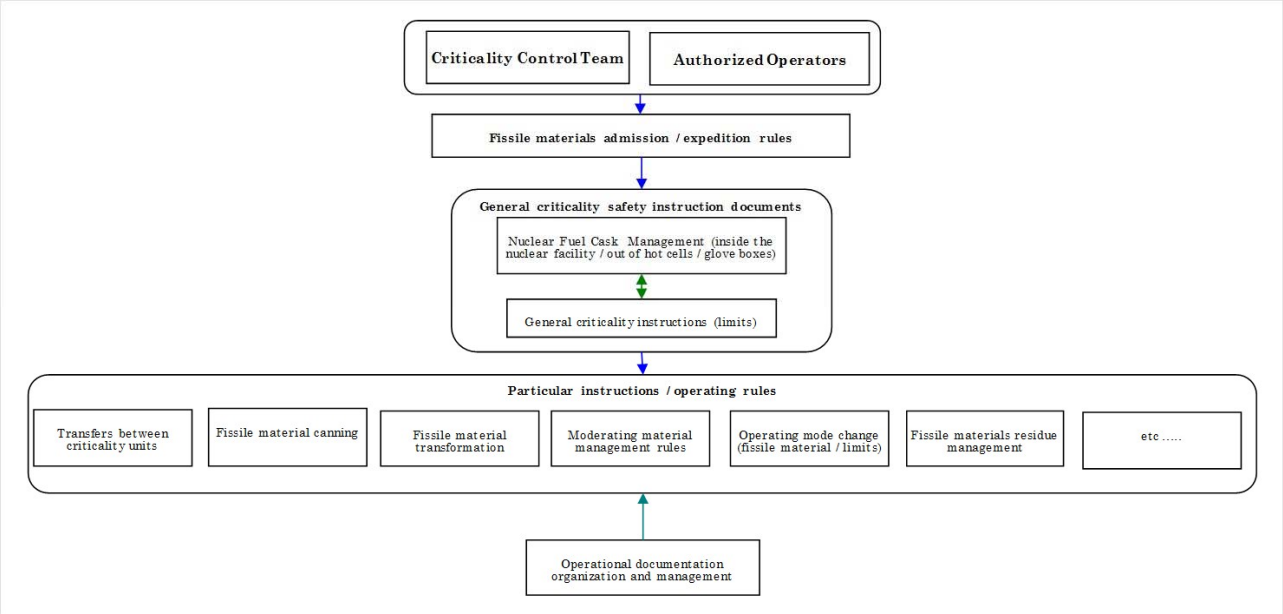

Figure I. Documentary organization

The handling of fissile materials in hot labs such as INB 55 is made through human intervention. No passive or active systems can be used because of the low fissile material flows between criticality units[2] (CU). Thus human/manual actions are part of the facility's safety report demonstration regarding sub-criticality, articulated through limits to be respected (i.e. mass of fissile material, quantity of moderating materials, etc.).
It is assumed that a human failure (clumsiness, misinterpretation of a situation, transcription error, etc.), related to the configuration of the criticality unit, the human relations in the organization and the personal or behavioural situation of an operator, can occur during one of these operations.
Concerning these anomalies of the "human error" type, an internal CEA recommendation states: *"If the same man has the possibility of causing two anomalies, it cannot be shown that they are independent. Consequently, regarding human errors, this rule requires that an operator must not be in a state leading to a criticality accident on his own".* So, in order to prevent criticality safety issues initiated by a human error, the operations related to criticality safety are subject to a criticality breakpoint formalized through the double control by two different persons (handlers/operators, officers).

b. <u>Organization for the implementation of the double control</u>

The organization initiated mid-late 2002, introduced a clear separation between the teams responsible for carrying out the operations (Operators, Handlers) and the teams in charge of controlling these operations (Controllers/Officers). The members of these teams (Operators/Controllers), were trained and subsequently formally authorized to execute the tasks related to criticality safety. This new organization ensures that a risk of criticality can arise only following the successive error of at least two different persons (for example: an operator and a controller in the case of a criticality regime change, and two operators and a controller when a movement between two CUs is executed).
Nowadays, this organization using the double control - prior to any action regarding criticality safety - is implemented in all the CEA / Cadarache nuclear installations, when this scheme is appropriate. It consists of:

- at the launch of the operation: a special record[3] is started by the operator(s) prior to the action presenting a criticality risk; he writes down the nature of the operation, the type of the fissile material, and the CUs concerned by the operation, the date, his name; finally he signs it;
- the criticality control team is convened to verify that the data provided by the operator(s) is consistent with the physical situation of the CU; the validity of the data indicated on the record is confirmed by the controller: he writes down his name, the date of the control and signs the record;

[2] The term "criticality unit" (unité de criticité) is currently used instead of the (ancient) term "work unit" in order to emphasize the importance of the geographical delineation regarding criticality safety.
3 In the case of a movement between two CUs, two cards are initiated: one at the sender CU, and another one at the receiver CU.

- the real operation action can be carried out within the limit of 24 hours following the controller's agreement, but in practice it takes place before the end of the shift. The operation's smooth running can be checked visually and with the process/production "tools" (modification of the nuclear material balance using the dedicated software, modification of the data on the criticality panels, etc.) by the control team; if the operations are not executed in due time the special record is barred and a explanation is annotated (for example: failure of an overhead crane prohibiting the operation).

The actions presenting a risk of criticality in INB 55 and subject to a double control are recalled in the following paragraph through a theoretical vision of the criticality lockdown during an action presenting a risk of criticality and its operational deployment on the installation.

5. OPERATIONS REQUIRING A DOUBLE CONTROL IN THE INB 55

The operations requiring double control in INB 55 can be grouped into 4 "theoretical configurations" of the activities presenting a criticality risk:

- Movement/transfer of fissile material from one CU to another having mass as one of the criticality control modes;
- Modification of the regime governing the criticality control modes or limits of a CU;
- Input/output of moderating materials in a CU when one of the criticality control modes is moderating material balance;
- Modification of the criticality operational limits (mass or number of items) through a repackaging of the fissile material into one sole container or a splitting of an item containing fissile material into several ones;

As it is impossible to perform a full description of the various situations encountered in the INB 55 we will only focus on the most usual/frequent operations presenting a criticality safety risk. These are the movements/transfers of fissile material and the moderating material management.

a. Movement of fissile material

Movements of fissile materials between two CUs are identified as criticality risk related actions. They are of many kinds:

- introduction of fissile material from another installation;
- transfer of fissile material from one CU to another;
- transfer of fissile material to or from storage.

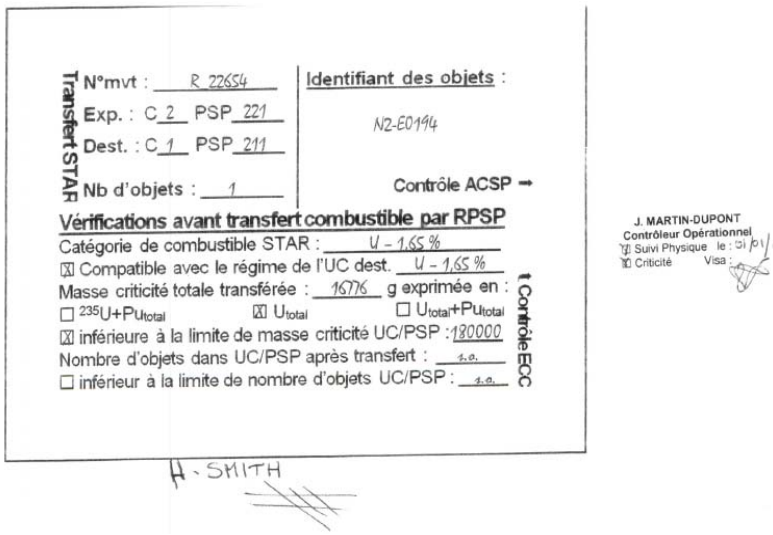
Transfert STAR
N°mvt : R 22654
Exp. : C 2 PSP 221
Dest. : C 1 PSP 211
Nb d'objets : 1
Identifiant des objets :
N2-E0194
Contrôle ACSP →
Vérifications avant transfert combustible par RPSP
Catégorie de combustible STAR : U - 1,65 %
☒ Compatible avec le régime de l'UC dest. U - 1,65 %
Masse criticité totale transférée : 16776 g exprimée en :
☐ 235U+Pu total ☒ U total ☐ U total+Pu total
☒ inférieure à la limite de masse criticité UC/PSP : 180000
Nombre d'objets dans UC/PSP après transfert : s.o.
☐ inférieur à la limite de nombre d'objets UC/PSP : s.o.
Contrôle ECC
J. MARTIN-DUPONT
Contrôleur Opérationnel
☒ Suivi Physique le : 01
☒ Criticité Visa :
H. SMITH

Figure II. Formalism of a movement / transfer between CUs

The transfer formalism shown on Figure II is about an object whose U_{total} mass is 16 776 g, with less than or equal to 1,65%, ^{235}U enrichment. This object is compatible with the mass limit of fissile material and number of objects of the receiving CU. The signatures of the operator/handler underneath and the controller/officer

aside of the form attest that the double control was realized before transfer. Other kinds of movements can be executed according to the same procedure.

b. Management of moderating materials

In order to ensure compliance with a mixed control mode including moderation, monitoring of moderating materials is carried out according to a procedure similar to movements of fissile materials.

INB 55 — FICHE DE GESTION DES QUANTITÉS DE MATÉRIAUX MODÉRATEURS LECA ET STAR
Fiche à initier et renseigner par le RC

Révision 3	☐ LECA ☐ STAR		
Fiche	n°	Cellule	C
Unité de criticité		Plan de travail	

MOUVEMENT								MATÉRIAU / OBJET					RÉGIME CRITICITÉ				VALIDATION	
Date	N° ordre chrono	Type de mouvement	Introduction en cellule — Origine (n° de cellule ou ZAR/Sas Sup…)	Mise en poubelle non scellée — Numéro de poubelle	Mise en poubelle non scellée — Rappel n° ordre entrée	Sortie de cellule ou poubelle scellée — Destination (n° de cellule ou ZAR/Sas Sup…)	Sortie de cellule ou poubelle scellée — Rappel n° ordre entrée et/ou n° de poubelle	Matériel à introduire (cf. liste dans CS 161)	Quantité à l'unité ou en : - mètre, - millitre, - gramme.	V_{EE} issu de CS 161	V_{EE} Autre (cf. PV) [4]	Volume Equivalent Eau total en ml	Cumul dans l'UC après mouvement en ml	Intitulé du régime criticité en cours	Limite modération[5] en ml	Cumul dans l'UC inférieur à la limite modération du régime ?	Responsable Cellule (nom et visa)	Contrôleur criticité[2] (nom et visa)
1/1/19	1	☐ Introduction ☐ Mise en poubelle scellée ☐ Mise en poubelle non scellée ☒ Sortie de cellule	5					flacon PE	100 g	200mL		200	1325	ω	/	☒ Oui ☐ Non	J. BOND	A. PANDRAGON
2/1/19	1	☒ Introduction ☐ Mise en poubelle scellée ☐ Mise en poubelle non scellée ☐ Sortie de cellule	5					lingettes	3	50mL		150	1475	ω	/	☒ Oui ☐ Non	J. BOND	L. ZAMBELLI

Figure III. Extract of the moderating material management special record

In conclusion, we can assert that from an organizational point of view, the double control as implemented in the INB 55, is in full compliance with the requirement for independence of the two anomalies (operator/handler error and defective verification by the controller/officer) so that the accident of criticality can be made possible. The DCP is therefore respected.

6. OPERATING FEEDBACK OF THE DOUBLE CONTROL AND THE CRITICALITY SAFETY ORGANIZATION IMPLEMENTATION IN THE INB 55

Since late 2002 and the establishment of the new organization in the INB 55/LECA-STAR facility in order to take into account the DCP through the double control, approximately 14,000 movements/transfers of fissile material presenting a criticality risk have been realized (nearly 4 per day); this number does not include the operations/controls related to the moderating material management for the CUs where moderation is one of the criticality control modes.[4]
In the past 16 years of operation, seven significant events regarding criticality safety were identified and reported[5]. The first three of them are unrelated to the double control and the DCP.

a. Event of January 24, 2006

This event concerns the inadvertent water flow into a cell of STAR. It occurred during the opening of a transport cask containing experimental PWR rods. The cask contained water following a default in the cask drying procedure before leaving the plant. A few liters of water flowed on the cell's ground. This event unrelated to the double control and the DCP, led however to a review of the cask reception conditions in the installation.

b. Event of October 25, 2009

This event concerns the discovery, during a clean-up campaign, of a quantity of hold-up fissile material superior to the authorized limit of the hot cell. The first estimates showed an excess of more than 6 kg of the uranium hold-up mass limit (estimate of 10 kg instead of the authorized 4 kg). The uranium handled in the cell was low enriched (75% of the material contained less than 1% of $^{235}U/U_{total}$, the maximum being 1.65%). The

[4] Between 2012 and 2014, during the destorage operations of the fissile materials in the MASURCA facility (MAquette SURgeneratrice de CAdarache) the double control was implemented as required by the DCP. Nearly 5,000 movements of fissile material (approximately 8 per day) were executed without a failure.
[5] The events can be found in the ASN internet site: https://www.asn.fr/.

total mass of uranium handled in the cell remained well below the critical mass, approx. 260 kg under unfavourable conditions.
The low enrichment fuel processes in the hot cell was completed in 2006 and the clean-up campaign was in progress. The double-control cannot be associated with the event because the hold-up is almost entirely attributed to the period preceding the implementation of the criticality safety organization (double-control and the DCP).

c. Event of November 21, 2012

This event is related to the discovery of fertile materials, during the inventory operations of the storage pits. These pits were filled between 1974 and 1981, the mass of fissile material accounted for was 0 g; this value is consistent with the standard criticality safety provisions considering fresh fuel composition even if it is an irradiated one. In this case it was fertile FBR fuel, so the fissile material balance after irradiation resulting from PIE's is 1%. The add up of these materials in the pit's fissile material balance resulted in exceeding the fissile material mass limit of the pit (infringement of a criticality safety limit as stated in the safety report). This event is unrelated to the double-control because initial DCP requirement [5] was initiated in 1984.

d. Event of Mars 6, 2014

This event is characterized by the transfer of a wrong can from one CU to another and by the non-respect of the double control. The event had no consequences, the wrong transferred can being identical in geometry with the right one and containing the same category of fissile material (control modes: mass and geometry). No criticality limits were reached, it would have required multiple human errors (multiple double control failures physically impossible in order to attain (eventually) a criticality accident. The event was detected by the next operator when he started his shift by initiating the double-control procedure. This implies that there are substantial organizational provisions and shows the robustness of the criticality safety organization.

e. Event of March 3, 2015

This event is characterized by the transcription of a faulty value of a fissile item's record that led to the non-compliance with a requirement of the safety report regarding moderating material. A can containing moderating material (2.7 liter of water equivalent) was placed on the cell's work surface where the volume of moderating material is limited to 0.5 liter of water equivalent.
No mass limits of the CU where exceeded. However, exceeding the quantity of moderating materials is an infringement of a criticality safety limit as stated in the safety report. This nonconformity was detected when the criticality safety officer performed data checking of the fissile material records during an inventory.

f. Event of November 28, 2017

This event is characterized by non-compliance with the criticality safety organization implemented in the INB 55. Two containers of fissile material were transferred between two CU in the facility. The handler/sender who initiated the material movement carried out also the control of the transfer data himself as handler/receiver. This an infringement of the general operating rules regarding criticality safety (separation between sender and receiver, which is the first part of the double control procedure). The event shows the importance of the formalization by a name and a signature to ensure that the double-control was actually applied.

g. Event of September 5, 2018

This event is characterized by the transfer from INB 55 (sender) to INB 50/LECI (receiver at the CEA/Saclay center) of fuel cladding sections (fuel cladding coming from the Phenix FBR) presumed having no fissile mass after their fissile pellets had been removed from the fuel pins. The criticality safety procedures were respected, the operators assumed the fuel clad was totally empty, but it wasn't. An extremely low mass of fissile material was trapped in the cladding. The event had no impact on criticality safety as verified a posteriori and safety issue of this event is quite low considering the quantities handled and the associated errors.

7. CONCLUSION

In terms of probability, only 4 events related to double control were identified in the INB 55/LECA-STAR after 16 years of implementation of the criticality safety organization using the double control as DCP. None of these events led to exit from the safe (or degraded) state as demonstrated the criticality safety analysis.
Moreover, the significant events encountered show that an error made by an operator/handler or a controller/officer, during a double-control (or even when it occurs in another context i.e. inventory operations), can be detected during the next operation in a CU, when the fissile material balance calculations are done prior to the movement authorization. This shows that the detection and correction time is adequate.

REFERENCES

[1] U.S. D.O.E. NCSP, https://ncsp.llnl.gov/training.php, Resources/Heritage videos, Heritage Video Conference 2000 Excerpt: The Double Contingency Principle",

[2] ANSI/ANS 8.1-2014, (R2018) November 29, 2018, American Nuclear Society, *nuclear criticality safety in operations with fissionable materials outside reactors,*

[3] IAEA Safety Standards, Specific Safety Requirements, No. SSR-4, S*afety of Nuclear Fuel cycle Facilities*,

[4] IAEA Safety Standards, Specific Safety Guide, No. SSG-27, *Criticality Safety in the Handling of Fissile Material,*

[5] Arrêté du 10 août 1984 relatif à la qualité de la conception, de la construction et de l'exploitation des installations nucléaires de base et *Règle fondamentale des sûreté* I.3.c, "criticité",

[6] J.O. – RF – no 278 du 2 décembre 2014, *Arrêté du 20 novembre 2014 portant homologation de la décision no 2014-DC-0462 de l'Autorité de sûreté nucléaire du 7 octobre 2014 relative à la maîtrise du risque de criticité dans les installations nucléaires de base,*

[7] GUIDE DE L'ASN – *Maîtrise du risque de criticité dans les installations nucléaires de base – Réalisé en partenariat avec* l'IRSN - Projet de GUIDE n°26. Version du 26 avril 2016,

[8] D. MIJUIN, H. CARROS, B. SEVESTRE. *The Organization of Criticality Hazard Prevention at the CEA.* ICNC 2003, **JAERI Conf, 2003 - 019**,

[9] G. KYRIAZIDIS - E. GAGNIER. *Nuclear criticality safety organisation at the Commissariat á l'Énergie Atomique et aux Énergies Alternatives*. IAEA Workshop on Criticality Safety, Vienna, 24-28, February 2014.

[10] G. KYRIAZIDIS - E. GAGNIER. *Criticality safety and organisation principles at the CEA.* OCDE – ORACS Workshop, Albuquerque, May 19-21, 2015.

[11] G. KYRIAZIDIS - E. GAGNIER – E. FILLASTRE. *Training Practices for CEA Engineers qualified in CRITICALITY SAFETY. ICNC 2015*, Charlotte, NC, September 13-17, 2015.

[12] O. DORVAL – D. NOYELLES – M. PRIGNIAU - G. KYRIAZIDIS – P. RIPPERT. "C*riticality safety analysis" training course for engineers to be qualified in criticality safety*. This conference, ICNC 2019.