



Septembre 2026

Rapport explicatif concernant la révision de mai 2027 de l'ordonnance sur l'énergie nucléaire

Table des matières

1. Présentation du projet1

2. Conséquences financières, conséquences sur l'état du personnel et autres conséquences pour la Confédération, les cantons et les communes1

3. Conséquences économiques, environnementales ou sociales1

4. Commentaires des dispositions1

1. Présentation du projet

En vertu de l'art. 2, al. 3, de l'ordonnance du 12 novembre 2008 sur l'Inspection fédérale de la sécurité nucléaire (OIFSN ; RS 732.21), l'Inspection fédérale de la sécurité nucléaire (IFSN) a l'obligation légale de faire vérifier périodiquement par des experts externes qu'elle répond aux exigences de l'Agence internationale de l'énergie atomique (AIEA). À l'automne 2023, une équipe internationale d'experts (le Service consultatif international sur la protection physique, IPPAS) a examiné la surveillance nucléaire suisse en matière de sûreté nucléaire. Dans son rapport rédigé en anglais¹, elle a formulé des recommandations et des suggestions. L'IFSN a conclu que la mise en œuvre de certaines de ces suggestions nécessitait une adaptation du cadre légal. Les modifications concernent notamment la distinction à faire entre la sécurité nucléaire et la sûreté, les responsabilités dans le domaine de la sécurité informatique² ainsi que la protection des installations nucléaires contre les cybermenaces. La sécurité informatique comprend en particulier la protection contre les cybermenaces et tient compte à cet égard des exigences concernant la sûreté des installations nucléaires et la sécurité nucléaire. Étant donné que la protection des systèmes d'information, des données et des infrastructures numériques contribue de plus en plus à garantir le fonctionnement sûr d'une installation nucléaire, des mesures de protection foncièrement fiables et solides doivent être mises en place.

Les modifications proposées consistent en des précisions et des compléments conformes aux normes internationales.

2. Conséquences financières, conséquences sur l'état du personnel et autres conséquences pour la Confédération, les cantons et les communes

Les modifications n'ont aucune conséquence sur les finances, l'état du personnel, ni d'autres conséquences pour la Confédération, les cantons ou les communes. Les adaptations prévues sont uniquement des précisions et des compléments concernant la surveillance nucléaire exercée par l'IFSN.

3. Conséquences économiques, environnementales ou sociales

Les modifications n'ont aucune conséquence sur l'économie, l'environnement ou la société. Elles reflètent la pratique actuelle. Elles n'ont aucune conséquence sur les finances ou l'état du personnel pour les exploitants d'installations nucléaires.

4. Commentaires des dispositions

Art. 9, al. 1^{bis}

Une des suggestions de l'équipe internationale d'experts concerne l'introduction de dispositions légales explicites relatives à la sécurité informatique (*computer security*) dans les installations nucléaires, ainsi

¹ *International Physical Protection Advisory Service (IPPAS), International Atomic Energy Agency (IAEA), IPPAS Follow-up Mission Report: Switzerland, 30 October - 10 November 2023*, (Service consultatif international sur la protection physique (IPPAS), Agence internationale de l'énergie atomique (AIEA), rapport final sur la mission de suivi concernant la Suisse, du 30 octobre au 10 novembre 2023).

² La sécurité informatique désigne la protection des systèmes d'information, des données et des infrastructures numériques contre les accès non autorisés, les manipulations, les défaillances et les utilisations abusives afin d'assurer la disponibilité, l'intégrité, la confidentialité et l'authenticité.

que la réglementation des responsabilités en la matière. Les experts recommandent de définir clairement les responsabilités de tous les acteurs impliqués afin de garantir une interprétation et application correctes de leurs obligations légales dans le domaine de la sécurité informatique. Cette suggestion est déjà en partie prise en compte dans la mesure où depuis l'entrée en vigueur, le 1^{er} avril 2025, de l'obligation de signaler les cyberattaques contre les infrastructures critiques, l'IFSN doit signaler à l'Office fédéral de la cybersécurité (OFCS) les cyberattaques contre une installation nucléaire qui remplissent les conditions prévues à l'art. 74d de la loi du 18 décembre 2020 sur la sécurité de l'information (LSI ; RS 128). Il manque toutefois encore une réglementation explicite de la responsabilité générale concernant la sécurité informatique dans les installations nucléaires.

L'art. 5, al. 3, de la loi fédérale du 21 mars 2003 sur l'énergie nucléaire (LENu ; RS 732.1) stipule que des mesures de sûreté doivent être prises notamment pour empêcher des tiers d'attenter à la sécurité des installations et des matières nucléaires. Cela comprend également les actes illicites touchant les systèmes informatiques ou informatisés d'une installation nucléaire qui compromettent la sécurité nucléaire. Cela signifie que la sécurité informatique d'une installation nucléaire fait partie intégrante de la sûreté et donc de la sécurité nucléaire au sens de la LENu.

L'art. 9 de l'ordonnance du 10 décembre 2004 sur l'énergie nucléaire (OENu ; RS 732.11) est donc complété par un alinéa 1^{bis}, qui mentionne explicitement la sécurité informatique dans les installations nucléaires comme un élément de la sécurité et de la sûreté. L'art. 6, let. a, OENu établit que l'IFSN est une autorité de surveillance pour la sécurité et la sûreté nucléaire. La compétence de l'IFSN pour la sécurité informatique est donc ainsi clairement définie.

Art. 9a

S'agissant des dispositions légales relatives à la sécurité informatique, l'équipe internationale d'experts a par ailleurs constaté que via la directive ENSI-G22³, l'IFSN a établi des principes essentiels en matière de sécurité informatique dans les installations nucléaires. Cette directive se fonde notamment sur les principes régissant la conception d'une centrale nucléaire (art. 10, al. 2, OENu) et des autres installations nucléaires (art. 12, al. 3, OENu). Les experts font toutefois remarquer qu'en Suisse, il n'existe actuellement pas de bases explicites juridiquement contraignantes dans ce domaine.

Le nouvel art. 9a introduit une disposition qui oblige les exploitants d'installations nucléaires à prévoir des mesures appropriées de protection contre les cybermenaces. Il charge également l'IFSN de préciser, dans des directives, les exigences à respecter à cet égard. De ce fait, il constitue une base légale explicite pour la directive ENSI-G22.

Le nouvel article se base sur l'art. 5, al. 3 et 4, LENu, qui prévoient que des mesures de sûreté doivent être prises pour empêcher des tiers d'attenter à la sécurité nucléaire des installations et des matières nucléaires et que le Conseil fédéral fixe les mesures nécessaires.

Art. 9b

L'AIEA aborde dans ses documents la distinction à faire entre la sécurité nucléaire et la sûreté. Les derniers documents qu'elle a publiés (par exemple les « Normes de sûreté » et la collection « Sécurité nucléaire ») comprennent tous une clause générale selon laquelle les mesures de sûreté (« safety ») et les mesures de sécurité (« security ») doivent être conçues et mises en œuvre de manière intégrée de sorte que les mesures de sécurité ne portent pas préjudice à la sûreté et que les mesures de sûreté ne portent pas préjudice à la sécurité (voir Agence internationale de l'énergie atomique, Principes fondamentaux de sûreté, n° SF-1, Vienne 2006, paragraphe 1.10).

Dans ce contexte, l'équipe internationale d'experts a constaté que la distinction entre les aspects liés à la sécurité et ceux liés à la sûreté était correctement appliquée dans la pratique par l'IFSN, mais qu'il

³ Directive ENSI-G22, « Sécurité informatique des installations nucléaires », édition de décembre 2019 (non publiée).

manquait une réglementation explicite au niveau de la loi ou de l'ordonnance. Dans la LENu, les mesures de protection sont décrites à l'art. 5 du chap. 2 « Principes de la sécurité nucléaire ». Les mesures de protection pour la sécurité nucléaire (al. 1 et 2) et pour la sûreté (al. 3) y sont traitées dans des alinéas distincts, sans toutefois qu'un lien entre elles soit établi. Dans l'OENu, les exigences pour la sécurité nucléaire figurent à l'art. 7 et celles pour la sûreté à l'art. 9, et cela qu'aucun lien ne soit établi entre elles non plus. Par ailleurs, l'art. 10 ne permet aucunement de faire la distinction entre la sécurité nucléaire et la sûreté.

Une réglementation juridique permettant de faire la distinction entre la sécurité nucléaire et la sûreté et de prendre en considération de manière intégrée les mesures qui relèvent de ces deux domaines de sorte que celles-ci ne se portent pas préjudice aide la Suisse à assumer ses responsabilités et à exercer sa surveillance conformément aux principes internationaux en vigueur dans le domaine nucléaire. Cette approche correspond également à la pratique internationale.

Art. 30, al. 4

L'accélération de la numérisation dans les installations nucléaires a considérablement accru l'importance de la sécurité informatique. Cette tendance devrait se poursuivre ces prochaines années. Dans la pratique, les exploitants d'installations nucléaires ont déjà mis en place des structures *ad hoc* au niveau de l'organisation et du personnel afin de définir clairement les responsabilités dans le domaine de la sécurité informatique. La présente adaptation de l'art. 30, al. 4, OENu tient compte de cette réalité en conférant une base légale à la pratique existante. Elle contribue ainsi dans une large mesure au renforcement de la sécurité nucléaire et de la sûreté.

Art. 36, al. 1, art. 62, let. a, et annexe 5

Selon l'équipe internationale d'experts, dans les dispositions légales, les termes « sécurité » et « sûreté » ne sont pas utilisés de façon compréhensible ni systématiquement délimités dans tous les articles. Il en ressort que les explications des dispositions laissent une marge d'interprétation, ce qui peut donner lieu à des divergences de vues et, partant, à une insécurité juridique potentielle. Il est donc recommandé de distinguer ces termes de manière rigoureuse et de les utiliser correctement dans les dispositions concernées.

C'est pourquoi, le terme « sûreté » est ajouté à des fins de précision à l'art. 36, al. 1, à l'art. 62, let. a, et à l'annexe 5, qui concerne le rapport mensuel, car ces dispositions portent sur les deux aspects, c'est-à-dire la sécurité et la sûreté.

L'art. 36, al. 1, dispose donc que le détenteur d'une autorisation d'exploiter doit suivre les résultats de la recherche et examiner dans quelle mesure il peut en tirer des enseignements non seulement pour la sécurité de son installation, mais aussi pour sa sûreté.

Dans le cas d'une demande d'autorisation générale pour un dépôt en couches géologiques profondes, le rapport à présenter conformément à l'art. 62 doit également couvrir l'aspect de la sûreté dans la comparaison des options envisageables. À noter que les pièces à fournir dans le cadre d'une telle demande, qui sont mentionnées à l'art. 23 OENu, article cité dans phrase introductive de l'art. 62, comprennent un rapport de sûreté (art. 23, let. a).

Selon l'annexe 5, le rapport annuel des installations nucléaires doit traiter de la même manière les aspects de la sécurité et de la sûreté. Par conséquent, ces deux aspects doivent également être pris en compte dans le rapport mensuel des centrales nucléaires sur l'exploitation de l'installation. Dans la pratique, le rapport mensuel comprend déjà actuellement des aspects liés à la sûreté. Par ailleurs, une correction est apportée à la dernière phrase de la ligne portant sur le rapport mensuel dans la version française de l'ordonnance.