

Computer security of nuclear power plant instrumentation and control systems. IAEA guidance versus the Polish legal framework on the eve of the first unit's construction

Cyberbezpieczeństwo systemów kontrolno-pomiarowych elektrowni jądrowej. Wytyczne MAEA a polskie ramy prawne u progu budowy pierwszego bloku

Artur Chlebicki

*Independent Researcher, Gdańsk, Poland (MSc Eng. in Computer Science, Gdańsk University of Technology) ·
ORCID 0009-0009-7304-0138*

Abstract: The instrumentation and control (I&C) systems of a modern nuclear power plant are fully digital, and their compromise may impair nuclear safety functions. The International Atomic Energy Agency has built a dedicated layer of guidance around this problem (the NSS 42-G implementing guide [21] and the NSS 17-T (Rev. 1) [20] and NSS 33-T [17] technical guidance), resting on four interlocking concepts: sensitive digital assets, computer security levels, computer security zones, and the defensive computer security architecture. A parallel family of IEC standards for the nuclear industry has emerged: IEC 62645 [18], IEC 62859 [16] and IEC 63096 [19]. This paper sets that architecture of requirements against the Polish legal order at the moment when the investor has filed its application for a construction licence and the President of the National Atomic Energy Agency has 24 months to decide. Analysis of the legal texts leads to the conclusion that computer security of nuclear I&C is governed in Poland by four regimes that arose independently of one another and have never been reconciled: the design-and-safety regime, in which the design requirements regulation [5] speaks almost exclusively of reliability and devotes a single phrase in § 90(6) to deliberate interference; the classified information regime, to which Article 36c(4) of the Atomic Law [1] refers systems supervising the technological process, together with accreditation carried out by the Internal Security Agency at the “secret” classification level; the physical protection regime, whose statutory design basis threat lists cyber-attack while the 2008 implementing regulation is silent on digital systems; and the national cybersecurity regime, which after the amendment of 23 January 2026 [9] covers the investor holding the principal decision as an important entity and names the operator of a nuclear power facility as an essential entity from the operating licence. Each regime has a different authority, a different logic and a different trigger point in the facility life cycle, and none introduces the concepts on which the IAEA methodology rests. The national cybersecurity regime reaches the project already, but with general management duties only. One practical consequence is singled out: the IAEA cautions that safety analysis is not sufficient to define computer security requirements because it does not address mal-operations caused by malicious acts, yet the Polish design regulation grounds those requirements precisely in reliability analysis. The paper proposes a coverage map of NSS 33-T elements against national provisions and identifies the gaps that can be closed without amending primary legislation. The work is a review and conceptual study based solely on analysis of published documents, standards and legal acts. It contains no original research, measurements or testing. The coverage assessment presented in Figure 5 does not derive from measurement; it is the author's expert judgement, calibrated against the content of the documents analysed.

Keywords: computer security, instrumentation and control systems, I&C, nuclear power plant, IAEA, NSS 33-T, IEC 62645, Atomic Law, national cybersecurity system, NIS 2, design basis threat.

Streszczenie: Systemy kontrolno-pomiarowe i sterowania (I&C) współczesnej elektrowni jądrowej są w całości cyfrowe, a ich kompromitacja może naruszyć funkcje bezpieczeństwa jądrowego. Międzynarodowa Agencja Energii Atomowej zbudowała wokół tego problemu odrębną warstwę dokumentów (przewodnik wdrożeniowy NSS 42-G [21] oraz wytyczne techniczne NSS 17-T (Rev. 1) [20] i NSS 33-T [17]), opartą na czterech powiązanych pojęciach: wrażliwych aktywów cyfrowych, poziomów bezpieczeństwa komputerowego, stref bezpieczeństwa komputerowego oraz obronnej architektury bezpieczeństwa komputerowego. Równolegle powstała rodzina norm IEC dla przemysłu jądrowego: IEC 62645 [18], IEC 62859 [16] i IEC 63096 [19]. Artykuł zestawia tę architekturę wymagań z polskim porządkiem prawnym w momencie, w którym inwestor złożył wniosek o zezwolenie na budowę, a Prezes Państwowej Agencji Atomistyki ma na decyzję 24 miesiące. Analiza tekstów aktów prawnych prowadzi do wniosku, że cyberbezpieczeństwo I&C obiektu jądrowego jest w Polsce regulowane przez cztery reżimy, które powstały niezależnie od siebie i nie zostały ze sobą uzgodnione: reżim projektowo-bezpieczeństwowy, w którym rozporządzenie o wymaganiach projektowych [5] mówi niemal wyłącznie o niezawodności, a działaniu celowemu poświęca jedno wyrażenie w § 90 pkt 6; reżim ochrony informacji niejawnych, do którego art. 36c ust. 4 Prawa atomowego [1] odsyła systemy nadzorujące proces technologiczny, wraz z akredytacją prowadzoną przez Agencję Bezpieczeństwa Wewnętrznego na poziomie klauzuli „tajne”; reżim ochrony fizycznej, którego ustawowe projektowe zagrożenie wymienia cyberatak, podczas gdy rozporządzenie wykonawcze z 2008 r. milczy o systemach cyfrowych; oraz reżim krajowego systemu cyberbezpieczeństwa, który po nowelizacji z 23 stycznia 2026 r. [9] obejmuje inwestora posiadającego decyzję zasadniczą jako podmiot ważny, a operatora obiektu energetyki jądrowej wymienia jako podmiot kluczowy od chwili uzyskania zezwolenia na eksploatację. Każdy z tych reżimów ma inny organ, inną logikę i inny moment uruchomienia w cyklu życia obiektu, a żaden nie wprowadza pojęć, na których opiera się metodyka MAEA. Reżim krajowego systemu cyberbezpieczeństwa obejmuje przedsięwzięcie już dziś, ale wyłącznie ogólnymi obowiązkami zarządczymi. Osobno wskazano konsekwencję praktyczną: MAEA zastrzega, że analiza bezpieczeństwa nie wystarcza do zdefiniowania wymagań bezpieczeństwa komputerowego, ponieważ nie obejmuje wadliwych działań spowodowanych aktami złośliwymi, a polskie rozporządzenie projektowe opiera te wymagania właśnie na analizie niezawodnościowej. Artykuł proponuje mapę pokrycia elementów NSS 33-T przez przepisy krajowe i wskazuje miejsca, w których lukę można zamknąć bez zmiany ustawy. Praca ma charakter przeglądowo-koncepcyjny: opiera się wyłącznie na analizie opublikowanych dokumentów, norm i aktów prawnych. Nie zawiera badań własnych, pomiarów ani testów. Zestawienie pokrycia przedstawione na rysunku 5 nie pochodzi z pomiaru, lecz jest oceną ekspercką autora, skalibrowaną względem treści analizowanych dokumentów.

Słowa kluczowe: cyberbezpieczeństwo, systemy kontrolno-pomiarowe, I&C, elektrownia jądrowa, MAEA, NSS 33-T, IEC 62645, Prawo atomowe, krajowy system cyberbezpieczeństwa, NIS 2, podstawowe zagrożenie projektowe.

1. Introduction

The Polish nuclear programme has entered a phase in which questions about computer security stop being theoretical. On 31 March 2026 the investor, Polskie Elektrownie Jądrowe (PEJ), filed an application with the President of the National Atomic Energy Agency (Państwowa Agencja Atomistyki, PAA) for a licence to construct a nuclear facility [24]. Under Article 39a(1)(1) of the Atomic Law, the President of the Agency issues a decision in such a case within 24 months of the day the application is filed together with the required documents [1]. The proceedings are under way as this text is being written.

The investment concerns the Lubiatowo-Kopalino site in the municipality of Choczewo, where three AP1000 reactors supplied by Westinghouse are to stand, with a total capacity of up to 3750 MWe. The schedule in the 2025 draft update of the Polish Nuclear Power Programme, directed to public consultation, foresees construction licences and the start of construction work, that is the first nuclear concrete, in 2028, with commercial operation of the successive units beginning in 2036, 2037 and 2038 [23]. The road to this point was long and has been described in

the literature [37, 49], but only now is the programme passing from planning into design.

A preliminary safety report accompanies the construction licence application. Under Article 36d(1) and (2) of the Atomic Law, the investor first carries out safety analyses, submits them to verification in which entities involved in developing the facility design may not take part, and draws up the report on the basis of their results [1]. This is the document in which the requirements placed on I&C systems take binding form, and this is the moment when they can still be shaped.

Why these dates matter for the subject of this article follows from a simple property of instrumentation and control systems: their security architecture is settled at the design stage, not during operation. The division into zones, the directions of data flow, the choice of platforms, the way boundaries between systems of different safety significance are realised: all of this is, in practice, irreversible once the design is closed. If computer security requirements are not set now, then in ten years they can at best be approximated with compensatory measures, in a facility where every modification of a safety-relevant system is a heavy, costly procedure requiring regulatory consent.

The starting point is the IAEA's observation that new nuclear facilities use highly integrated digital I&C systems to handle very large volumes of process data simultaneously, with less human involvement than in previous-generation designs [17]. The same feature that yields the efficiency gain creates an attack surface that facilities designed in the 1970s simply did not have.

The aim of this article is to set the architecture of requirements that the IAEA and the IEC have built around I&C computer security against what Polish law says on the matter, and to point to the places where the two layers fail to meet. The thesis I put forward is this: Polish regulation addresses the computer security of a nuclear facility in four places, but each of those places speaks a different language and answers to a different authority. Together they do not add up to a coherent computer security programme in the sense that NSS 42-G gives that term [21].

2. Scope, method and limitations

This article is a review and conceptual study. Its material consists of published documents: IAEA guidance from the Nuclear Security Series, standards of the International Electrotechnical Commission, Polish legal acts together with their consolidated texts, and peer-reviewed literature. I checked every act of Polish law in the official ELI repository maintained by the Chancellery of the Sejm, which records the title, the promulgation address, the status in force and the full text. The quoted passages of statutes and regulations were read in the original, not through secondary accounts.

What this text does not contain needs saying at the outset. There are no original studies, measurements, penetration tests or analyses of specific installations. Nor is there any information about vulnerabilities of the Polish project, partly because none is public, and partly because publishing such things would be irresponsible regardless of their availability. Every number in the text comes from a cited document and is marked as such.

One point requires a separate reservation. Figure 5, discussed in section 8, presents the elements of the NSS 33-T guidance set against their coverage by national provisions. It is not the result of measurement or of a computational method. It is the author's expert judgement, calibrated against the content of the documents analysed, and as such it is open to debate. I offer it because without such a juxtaposition the scale of the difference is hard to show, but the reader should treat it as an argument, not as a measurement.

The author is a cybersecurity practitioner, not a nuclear engineer. The perspective of this text is that of protecting industrial process control systems, carried over onto the ground of nuclear regulation with all the caution such a transfer demands.

3. Why nuclear facility I&C is a special case

Transplanting office IT practice into control systems ends badly, and the industry literature has described this many times [30, 50]. In a nuclear facility the differences are sharper still.

The first difference is that the order of protection goals reverses. In information systems, confidentiality usually comes first. In I&C, what matters above all is the integrity of the signal and the availability of the function: a false temperature reading, or a blocked reactor trip signal, is a problem of a different category from a leaked document. The IAEA states this outright, listing the consequences of compromise of an I&C function in order from the worst: the function remains undetermined, with the effects of compromise producing an unnoticed change in the design or operation of the system; the function behaves unexpectedly but observably for the operator; the function fails; the function performs as expected, meaning the compromise does not affect it adversely [17, para. 2.21]. The worst case is not failure but a silent change in system behaviour that nobody notices. Detecting precisely such changes is a research strand of its own, covering methods for detecting falsified process signals [46, 53].

The second difference is the length and rigidity of the life cycle. An I&C platform chosen at the design stage operates for decades. A software update in a protection system is not a routine action but a modification that requires verification and validation to be repeated. The "patch fast" habit of general IT is here not so much difficult as formally prohibited without the proper procedure. This also shapes the way security testing can be performed, which must be subordinated to the operational regime of the facility [47].

The third difference, the least obvious one, is that a security measure can itself become a hazard to nuclear safety. The IAEA devotes a separate block of guidance to it. A badly designed protective measure can introduce new failure modes into the system, increase the probability of spurious actuation and undermine the system's ability to perform its safety function reliably; the example given is improperly implemented antivirus protection inside an I&C system, which adds complexity, adds latency and itself creates a new attack path [17, para. 3.37]. The guidance distils this into a rule: neither normal nor abnormal operation of any computer security measure should adversely affect the ability of the I&C system to perform its safety function [17, para. 3.44]. The failure modes of the protective measures themselves are to be identified, documented and included in the system hazard analyses [17, para. 3.45]. The OECD Nuclear Energy Agency reached similar conclusions when analysing the impact of cybersecurity features on digital safety systems [48].

The resolution of the conflict is unambiguous, and it is sometimes quoted inaccurately, so I quote it precisely. If

a conflict arises between nuclear safety and security, the solutions adopted for nuclear safety are maintained, but the operator is to seek a solution that complies with the computer security requirements; compensatory measures reducing the risk to an acceptable level are to be implemented, supported by full justification and risk analysis, and they should not rest solely on administrative measures for an extended period. The sentence closing that paragraph reads: the absence of a security solution should never be accepted [17, para. 3.49]. Nuclear safety wins the dispute over a particular measure, but it releases no one from the duty to secure the system.

This relationship has a standard of its own. IEC 62859 [16] deals exclusively with coordinating nuclear safety and cybersecurity: it is meant to optimise the introduction of cybersecurity provisions into I&C architectures and systems, to prevent conflicts between the two, and to help identify and exploit synergies. It is built of three parts: the I&C architecture as a whole, the level of the individual system, and organisational and procedural matters.

4. The IAEA requirements architecture

4.1. The document hierarchy

The IAEA guidance on computer security is layered. I reconstruct the layers here, because they decide which document governs what (Fig. 1).

At the top stand the Nuclear Security Fundamentals and the Recommendations. These include above all NSS 13, the recommendations on the physical protection of nuclear material and nuclear facilities known as INFCIRC/225/Rev. 5 [11], and NSS 20, which defines the objective and essential elements of a state's nuclear secu-

rity regime [12]. Below them sits the implementing guide NSS 42-G [21], issued in 2021. It is the first IAEA document to cover computer security as a whole: the roles of the state and of entities, the national strategy, the elements of computer security programmes and the sustaining activities. Lower still lie the technical guidance documents: NSS 17-T (Rev. 1) on computer security techniques for nuclear facilities [20], issued in 2021 as a revision of the 2011 document, and NSS 33-T of 2018 [17], devoted solely to I&C systems. The division of labour between these two is distinct: NSS 17-T (Rev. 1) describes computer security risk management at the level of the whole facility, from defining the scope and characterising the facility, through threat characterisation, to the specification of requirements [20, para. 4.10]. NSS 33-T descends to the level of the individual I&C system and its life cycle. NSS 42-G itself describes this relationship, referring the reader to NSS 33-T and NSS 17-T (Rev. 1) for more detailed guidance, examples of the technical implementation of measures, and risk management. The set is completed by NSS 23-G on the security of nuclear information [13] and by the documents on the design basis threat [22] and on nuclear security culture [10].

For a practitioner the most important document is NSS 33-T, because it is the only one in this family written specifically for instrumentation and control systems. Its guidance is arranged in four chapters: key concepts, the risk-informed approach, the I&C system life cycle, and activities in the individual phases of that cycle; the last of these chapters alone runs to 226 numbered paragraphs. Its counterpart on the nuclear safety side is SSG-39, on the design of I&C systems for nuclear power plants [14], and on the management side, GSR Part 2 [15].

One thing has to be noted here, and it matters to anyone who wants to rely on these documents in licensing

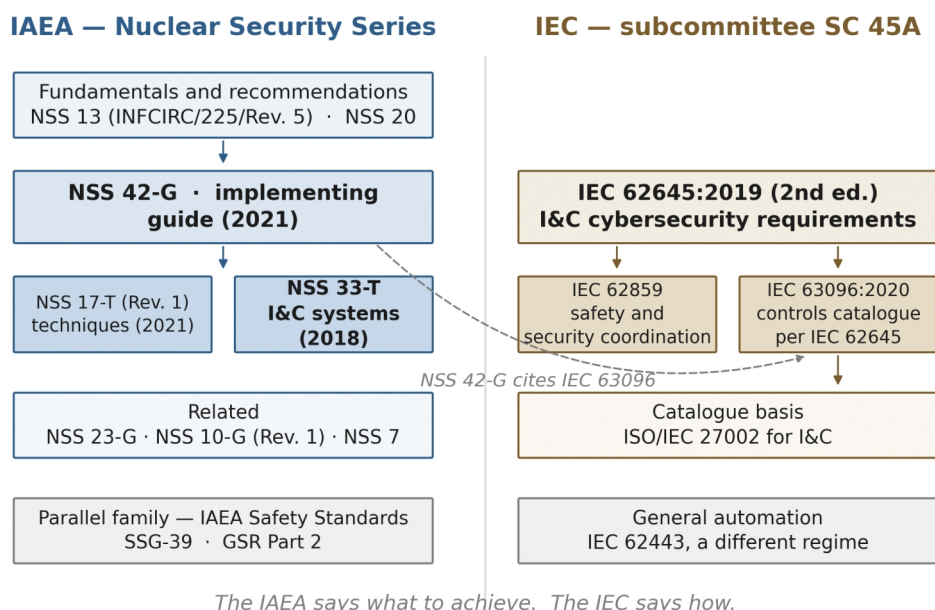


Fig. 1. The hierarchy of IAEA documents and IEC standards on the computer security of nuclear facilities. Author's own elaboration based on the content and reference lists of NSS 42-G [21] and NSS 33-T [17] and on the descriptions of IEC 62645 [18], IEC 62859 [16] and IEC 63096 [19].

proceedings. NSS 33-T dates from 2018, and its reference list still cites NSS 17 of 2011 and IEC 62645:2014, both of which have since been superseded. A revision of NSS 33-T is in preparation. Invoking this document in design documentation therefore requires checking that the standards it cites onward are not already outdated. The earlier edition of NSS 17 was, for that matter, the subject of a critical analysis of attack scenarios, which pointed to the limitations of the approach as it then stood [27].

4.2. Four load-bearing concepts

The whole IAEA methodology rests on four concepts that hold one another up. I give the definitions after the NSS 42-G glossary [21].

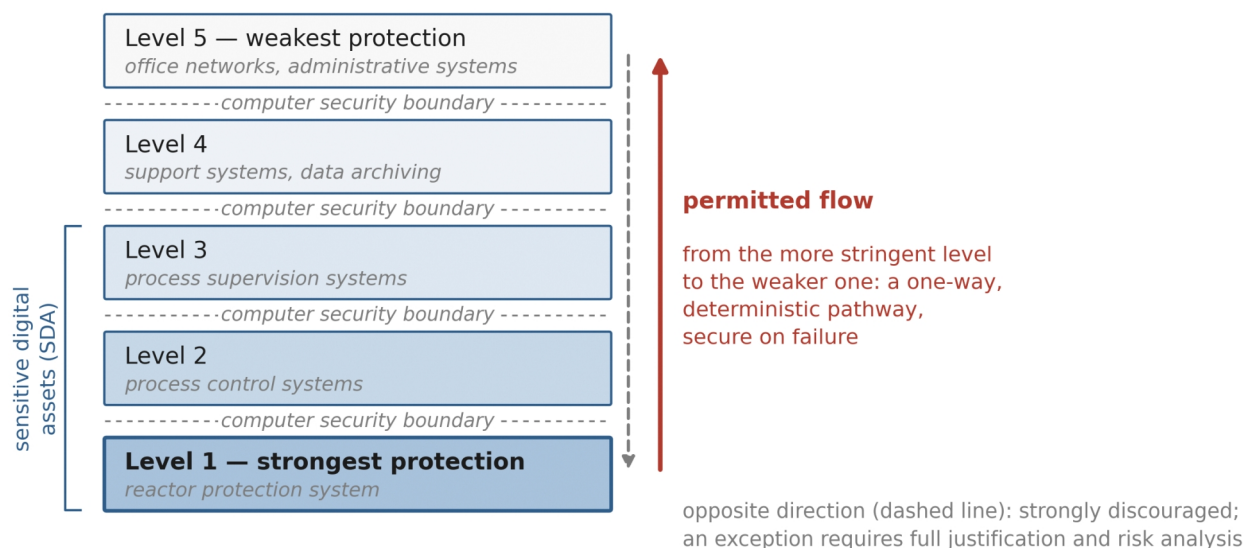
Sensitive digital assets (SDA) are sensitive information assets that are computer-based systems or parts of such systems. Sensitive information assets comprise any equipment or components used to store, process, control or transmit sensitive information, including control systems, networks and information systems. Identifying SDAs is the first step: until it is known what is being protected, the later stages have no foundation.

A **computer security level** is the strength of protection required to meet the computer security requirements for a function associated with physical protection, nuclear safety, nuclear material accounting and control, or the management of sensitive information. NSS 17-T (Rev. 1) gives a concrete scale: levels are numbered from 5, requiring the weakest protection, to 1, requiring the strongest, with systems containing sensitive digital assets placed at levels 1 to 3, and the remaining digital assets at levels 4 and

5 [20, para. 3.24]. Requirements attach to the level, while the choice of a specific measure remains a design decision, dependent on the architecture and technology of the asset concerned [20, para. 3.23]. NSS 33-T stresses at the same time that computer security levels and nuclear safety classes are distinct, though related, concepts [17, para. 2.24]. The operator assigns the level on the basis of the potential consequences of failure or malfunction of the system, including behaviour departing from the design or from the failure modes assumed in the safety analysis. The level is a property of the system itself and does not depend on its environment [17, para. 2.27]. Practical experience of categorising I&C systems by level has been described by the Ukrainian nuclear regulator in a series of articles [28, 32, 35, 42], one of the few public accounts of this process from a regulator's perspective.

A **computer security zone** is a group of systems with common physical or logical boundaries that have been assigned a common computer security level in order to simplify administration, communication and the application of protective measures. All systems in a zone are protected at the most stringent level present in that zone [17, para. 2.28]. The consequence is practical: a communication device performing functions of low significance, but placed in the zone of the reactor protection system, receives that system's level, because it can be used to compromise it [17, para. 2.30].

The **defensive computer security architecture** binds the above into a design solution. The operator is to define an overall defensive architecture in which every I&C system has an assigned level and is protected in accordance with the corresponding requirements [17, para. 4.132]. The



Measures at the boundaries of neighbouring levels use different technologies.

Remote access to the most stringent level is impossible in this construction.

Fig. 2. Computer security levels, zones and data flow rules in the defensive computer security architecture. A conceptual diagram based on NSS 17-T (Rev. 1) [20], para. 3.24 (the five-level scale and the placement of sensitive digital assets), and NSS 33-T [17], paras 2.28–2.30 and 4.132–4.143 (zones, boundaries, flow rules). The assignment of specific systems to levels is an example illustrating the rule, not a depiction of any real installation.

architecture is to make it possible to prevent attacks, detect them, delay them, mitigate their consequences and recover from them [17, para. 4.133].

4.3. Architecture rules and defence in depth

Several construction rules follow from the architecture chapter. They are what translates the concepts into design decisions (Fig. 2).

Computer security boundaries are introduced between systems of different levels [17, para. 4.134], and data flow between zones of different levels, as well as between systems within the same level, is subject to control based on risk assessment [17, para. 4.135]. Systems at the highest level are connected to systems at lower levels only through one-way, deterministic communication pathways operating in a fail-secure mode, with the direction of flow restricted to transmission from higher-level systems to lower-level systems; exceptions are strongly discouraged and may be considered only case by case, with full justification and risk analysis [17, para. 4.136]. The document notes on this occasion that some Member States take the view that exceptions should not be allowed at all. Remote access to systems at the highest level is impossible in this construction, which follows directly from the one-way restriction on outbound traffic.

Technical measures applied inside a zone or at its boundary are to use technologies different from those applied at neighbouring levels and boundaries, which provides diversity of protection [17, para. 4.140]. Wireless communication in systems at the most stringent level is considered problematic, because a secure boundary is difficult to assure for it [17, para. 4.138].

Defence in depth against compromise is, in this methodology, more than technical layering. It consists of multiple layers of measures that must fail or be bypassed for an attack to progress, but it also includes maintaining a programme of measures that assess, prevent, detect, protect, respond, mitigate and recover [17, para. 4.142]. The requirement closing this block is a strong one: no single failure within or between the defensive layers should invalidate the protection as a whole [17, para. 4.143]. This carries over to security the same principle that nuclear safety described long ago and in detail [31], with the difference that here the layers face an adversary rather than a probability distribution. The design of systems robust against compromise has also received dedicated treatment [44].

4.4. The graded approach

The IAEA requires requirements to be graded according to risk, and it says what is to be taken into account: the significance of the I&C system's function both for nuclear safety and for security; the identified and assessed threats

to the facility; the attractiveness of the system to a potential adversary; the vulnerabilities of the system; the operating environment; and the potential consequences that compromise of the system could cause, directly or indirectly [17, para. 2.20]. Requirements are defined in proportion to the potential consequences of an attack [17, para. 2.21].

Two items on that list have no counterpart in purely reliability-based thinking: attractiveness to an adversary, and threat assessment. Reliability asks how often something fails. Security asks who would want to break it, and why. These are different questions, and they lead to different designs.

The IAEA says as much directly when listing the inputs to computer security risk management for a facility. Among them is the safety analysis of the facility's computer systems, with a caveat: that analysis may serve to define computer security requirements, but it is not sufficient for the purpose, because it does not cover all mal-operations, in particular those caused by malicious acts [20, para. 4.9]. I return to this caveat in section 7, in assessing the Polish design regulation. The literature supplies tools for ordering this second perspective: a taxonomy of attacks on the digital environment of a nuclear power plant [40] and a framework for assessing attack scenarios by relative difficulty of execution and consequence [41].

5. The IEC family of standards

The IAEA guidance describes what is to be achieved. The IEC standards describe how to do it in engineering terms, and they form a coherent family prepared by subcommittee SC 45A (Fig. 1). Their genesis and mutual relations are discussed at greater length in the literature [43, 51].

IEC 62645 [18] is the base document. The second edition, of November 2019, replaced the 2014 edition and changed the title along the way: from requirements for security programmes for computer-based systems to cybersecurity requirements for instrumentation, control and electrical power systems of nuclear power plants. The standard establishes requirements and guidance for developing and maintaining computer security programmes for programmable digital I&C systems, and it defines measures for preventing, detecting and responding to malicious acts committed by digital means. It is the source of the concept of security degrees, to which the other standards of the family refer.

IEC 62859 [16] is responsible for coordinating nuclear safety and cybersecurity, as discussed above.

IEC 63096 [19], of October 2020, supplies a catalogue of security controls, recommended and optional, graded according to the security degrees defined in IEC 62645. The catalogue builds on the controls of ISO/IEC 27002, with the original requirements modified, refined or sup-

plemented where this proved necessary from the perspective of programmable digital I&C systems. The standard addresses both the I&C of new plants and the modernisation of existing facilities. It is also the standard the IAEA cites in NSS 42-G when discussing security measures.

The construction of this family has one distinct advantage: it avoids carrying over wholesale the provisions of IEC 62443, which was written for industrial automation in general [26]. The zone-based approach is similar in both families [57], but the nuclear requirements take account of safety classification, qualification requirements and a modification regime that general automation does not have. A separate issue, beyond the scope of this article, is the interface between a nuclear power plant and the power system, and the couplings that follow from it [45].

6. What the documented incidents teach

Incidents call for caution, because accounts circulate in this field that do not survive confrontation with the source. I confine myself to what the operator confirmed or what peer-reviewed analysis established (Fig. 3). A broader treatment of the cases from a nuclear security perspective can be found in a handbook chapter [52].

Stuxnet (2010) remains the reference case, because it showed that malicious software can be written for a specific configuration of industrial controllers and can alter the behaviour of the process while presenting the supervision system with a picture of normal operation [25]. Its significance for nuclear regulation is twofold. It demonstrated that separating a network from the Internet is not a safeguard in itself. It also enacted precisely the worst-case scenario the IAEA describes as an unnoticed change in the operation of a system. The IAEA cites an analysis of this case as the first item in the NSS 33-T reference list.

Korea Hydro and Nuclear Power (2014) is the case in which reactor documentation, manuals and employees' personal data leaked, the entry vector being the phishing of people connected with the operator and its subsidiaries. Control systems were not breached [33]. The lesson is therefore not a direct threat to unit operation but something subtler: the design documentation of I&C systems is itself a sensitive asset, because it shortens an adversary's path to preparing an attack. That is exactly how the IAEA defines sensitive information and sensitive information assets [13, 21].

Kudankulam (2019) supplied the case of malicious software present in the administrative network of a power plant. The operator, Nuclear Power Corporation of India, confirmed on 30 October 2019 that malware had been detected. It concerned, according to the operator, a single computer connected to the administrative network; the operational networks controlling the two 1000 MW units are entirely separate from it [36]. With all due caution towards operators' statements, the case illustrates the IT-OT boundary as the real point at which the scale of an incident is decided, and it is an argument for that boundary being designed rather than assumed.

The common lesson of these three cases is that network separation works exactly as well as it was designed and is maintained. The literature has described mechanisms for carrying data across the boundaries of networks assumed to be isolated [34]. The IAEA addresses this directly, requiring that removable media, portable devices and other temporary equipment that needs access to a system be used only within a single zone or a defined set of zones [17, para. 2.29]. A separate thread, not developed here, is the insider threat, which has its own literature [29, 54] and its own IAEA documents.

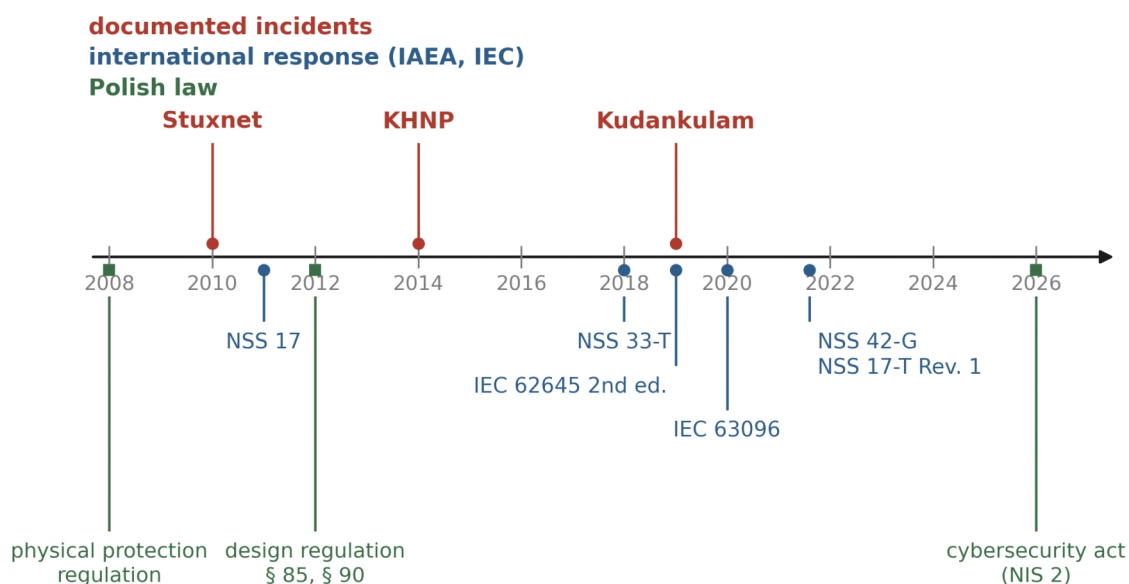


Fig. 3. Chronology of documented incidents relevant to the computer security of nuclear facilities and of the regulatory response. The compilation includes only incidents confirmed by the operator or described in peer-reviewed literature [25, 33].

7. The Polish legal framework

Set against the above, national law can be summarised in one sentence: the computer security of nuclear facility I&C is regulated in Poland in four places, which came into being independently and have never been reconciled with one another (Fig. 4).

7.1. The first regime: design requirements

The basis is the Regulation of the Council of Ministers of 31 August 2012 on the nuclear safety and radiological protection requirements to be taken into account in the design of a nuclear facility [5]. It devotes two provisions to ICT systems (systemy teleinformatyczne).

Paragraph 85 concerns the situation in which the correct operation of a system important to nuclear safety and radiological protection depends on the reliable functioning of an ICT system. It then requires appropriate standards and procedures to be implemented and applied throughout the period of the system's use, in particular in the software development cycle. Subparagraph 2 requires the reliability level of the hardware and software to be commensurate with the importance of the system for the fulfilment of safety functions. Subparagraph 3 requires the adopted reliability level to include safety margins compensating for the uncertainties of analysis arising from the complexity of the system.

Paragraph 90 adds six requirements for ICT systems used in safety systems, in particular in the protection system: high quality requirements commensurate with the significance of the system; systematic documentation and review of the development process, together with the control, testing and acceptance of design changes; confirmation of high reliability by a specialist independent of the

designer and the supplier; diverse technical solutions where safety functions are of fundamental significance for reaching and maintaining safe shutdown; consideration of common cause failures caused by software errors; and, in point 6, the introduction of protection against accidental or deliberate interference (zabezpieczenia przed przypadkową lub rozmyślną ingerencją) with the operation of the system.

The proportions of these provisions speak for themselves. Five of the six requirements of § 90, and the whole of § 85, concern quality and reliability: the development cycle, documentation, independent verification, common cause failures. That is the language of safety engineering, and on its own terms it is sound. Intentional action receives a single expression: the word “deliberate” (rozmyślną) in point 6, in a sentence that places it beside accidental interference. For comparison, NSS 33-T develops the same subject matter across four chapters of numbered guidance, of which the chapter on life-cycle activities alone contains 226 paragraphs, and IEC 63096 supplies a full catalogue of controls. I am not arguing that the design regulation should contain such a catalogue; that is not its role. I am arguing that a single adjectival aside does not create a basis on which a regulator could assess a defensive computer security architecture, because it defines neither the concepts nor the criteria.

Here the IAEA caveat quoted in section 4.4 returns. Safety analysis of a facility's computer systems is not sufficient to define computer security requirements, because it does not cover mal-operations caused by malicious acts [20, para. 4.9]. The Polish design regulation does exactly what that paragraph warns against: it builds the requirements for ICT systems solely on the ground of reliability analysis. This bears directly on the licensing proceedings, because the preliminary safety report is drawn up precisely

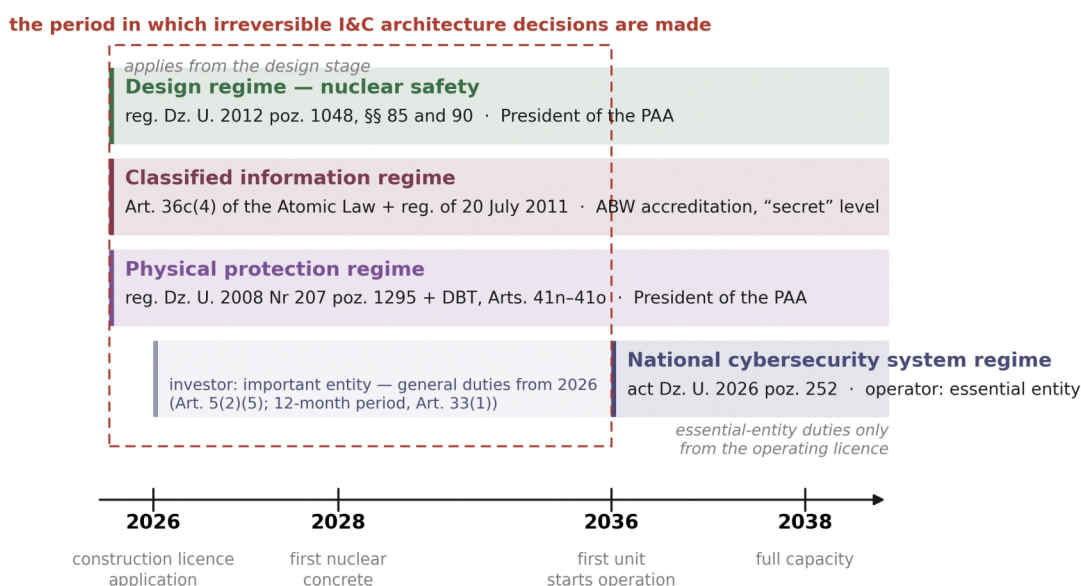


Fig. 4. The four regulatory regimes applicable to the computer security of nuclear facility I&C in Poland, set against the phases of the facility life cycle. Author's own elaboration based on the texts of the legal acts [1, 2, 5, 9]. Schedule dates after the 2025 draft update of the Polish Nuclear Power Programme [23].

on the basis of the safety analyses conducted under Article 36d(1) of the Atomic Law [1].

What these provisions do not contain is telling as well. There are no computer security levels, no zones, no requirement to identify sensitive digital assets, no one-way data flow rule, no requirement of diverse technologies at zone boundaries. There is also no obligation to take a threat assessment into account when defining the requirements for a system, and that is precisely the element that distinguishes security from reliability.

7.2. The second regime: protection of classified information

The second place is Article 36c(4) of the Atomic Law [1]. The provision states that ICT systems forming elements of the critical ICT infrastructure (teleinformatyczna infrastruktura krytyczna) intended for supervising the course of the technological or production process in nuclear facilities are designed, built and operated in a manner meeting the ICT security requirements laid down in the provisions on the protection of classified information for systems and networks used to process classified information bearing the “secret” (tajne) classification. The authority competent for the accreditation of these systems and networks is the Internal Security Agency (Agencja Bezpieczeństwa Wewnętrznego, ABW).

This is the only provision in Polish nuclear law that places real, enforceable ICT security requirements on the systems supervising the technological process, together with a procedure for confirming them. Its construction deserves attention, though, because it has three consequences.

The first concerns the logic of the requirements. The classified information regime exists to prevent disclosure, but its technical layer is broader than confidentiality alone. The requirements to which Article 36c(4) refers are laid down in the Regulation of the Prime Minister of 20 July 2011 on basic ICT security requirements [4]. Its § 5(1) obliges the protection of confidentiality, integrity and availability alike; § 5(2) requires risk management, limited trust towards other systems, layered protection and security testing; § 18 spans the entire period of the system’s operation; and § 20 requires the identification of resources, threats, vulnerabilities and safeguards. Read together with the accreditation procedure, this is a real security-management regime, not an access-control annex. What it is not is an I&C regime. It grades nothing by the consequences of a compromised control function, and it knows none of the NSS 33-T concepts: no levels, no zones, no defensive architecture, no one-way data flows. Accreditation at the “secret” level therefore covers more of the NSS 33-T problem than a confidentiality-only reading would suggest; it still does not cover the whole of it.

The second concerns scope. The provision covers systems intended “for supervising the course of the technological or production process”. The IAEA methodology covers all systems whose compromise could adversely affect nuclear safety or security, together with the principle of assigning auxiliary devices to the level of the zone in which they are placed [17, para. 2.30]. A scope based on the supervisory function and a scope based on the potential consequences of compromise do not coincide.

The third concerns the authority. Accreditation is carried out by the ABW, an authority other than the President of the PAA, who approves the physical protection system and issues licences. NSS 42-G discusses the division of roles between the state and the operator and underlines the need for coherence of the whole regime [21]; the dispersal of competences is not a defect in itself, but it calls for a coordination mechanism.

7.3. The third regime: physical protection and the design basis threat

Physical protection is a regime in its own right: it has its own authority, its own approval moment and its own logic. It is also where the IAEA places computer security: NSS 13 treats it as an element of facility protection [11].

The Polish Regulation of the Council of Ministers of 4 November 2008 on the physical protection of nuclear material and nuclear facilities [2], still in force, contains not a single reference to ICT, computer or information systems. I checked this directly in the text of the act. The regulation dates from 2008, which is to say before Stuxnet, before NSS 17 and before the entire layer of IAEA documents described in section 4. This is the most direct gap and, at the same time, the easiest to close, because closing it does not require amending the statute.

The statute itself is more modern in this respect than its implementing act. The definition of the design basis threat contained in the Atomic Law includes the characteristics of entities that may seek to commit acts such as theft, unauthorised use, cyber-attack, an act of terror or sabotage, and this threat is taken into account in developing the physical protection system [1]. The statute requires the design basis threat to be taken into account in the development, approval and review of physical protection systems (Article 41n), and it is drawn up by the President of the PAA in consultation with the competent authorities (Article 41o), which corresponds to the construction recommended by the IAEA [22]. The current revision of that guidance, NSS 10-G (Rev. 1) of 2021, matters here in its own right: it brings computer security into the national threat assessment and sets out, step by step, how a design basis threat that includes cyber threats is developed, maintained and used [22]. The bridge between the statutory mention of cyber-attack and a working, cyber-inclusive design basis threat therefore already exists at the method-

ological level. The President of the PAA also has, within the scope of oversight, the right to demand access for inspection to the networks or ICT systems used in the physical protection system of the inspected facility.

We therefore have a situation in which the statute lists cyber-attack among the design basis threats and gives the regulator an inspection tool, while the implementing act defining the content of physical protection is silent about digital systems. The statutory basis for filling this gap already exists.

7.4. The fourth regime: the national cybersecurity system

The fourth place is the newest. The Act of 23 January 2026 amending the Act on the National Cybersecurity System and certain other acts [9], promulgated on 2 March 2026, implements the NIS 2 Directive [8] by amending the 2018 statute [7]. Under its Article 49, it enters into force one month after the day of promulgation, that is on 3 April 2026.

Three of its elements matter for the subject of this article. In Annex 1, covering the essential sectors, a subsector “Nuclear energy” has been distinguished within the Energy sector. The type of entity indicated is an entity operating a nuclear power facility within the meaning of the Act on the preparation and implementation of investments in nuclear power facilities and associated investments [3]. The statute also fixes the moment at which the operator of a nuclear power plant becomes an essential entity. It is the day it obtains the operating licence referred to in Article 4(1)(2) of the Atomic Law, or the day it obtains a concession for the generation of electricity or heat under the Energy Law, whichever comes first.

The operator is not the only addressee. Under Article 5(2)(5) of the amended statute, an investor for a nuclear power facility which has obtained the principal decision is an important entity, regardless of its size, and Annex 2 lists the corresponding sector, investments in nuclear power. Article 8 attaches the obligations of chapter 3 to essential and important entities alike, and under Article 33(1) of the amending act an entity that met the criteria on the day the amendment entered into force has twelve months to implement them. The investor obtained the principal decision in July 2023, before filing the construction licence application [24], so it met those criteria on 3 April 2026 and its general cybersecurity obligations fall due within a year of that date.

The nuclear programme thus enters the national cybersecurity regime explicitly, on two tracks: the investor as an important entity now, the operator as an essential entity from the operating licence. That is a qualitative change from the previous state. It does, though, raise the question of what each track carries, and when.

The two tracks differ in content. The investor’s obligations are the general management duties of chapter 3: a security management system, risk analysis, incident handling, documentation. They bind the investor as an organisation, and none of them speaks the language of I&C: no sensitive digital assets, no computer security levels or zones, no defensive architecture, no data flow rules. The operator’s obligations, attached to the essential-entity status, arrive with the operating licence or the concession, which on the current schedule means around 2036 [23]. By then the facility will have gone through commissioning, whose requirements a separate regulation governs [6], and the I&C systems will already be installed and tested. So the regime reaches the project today, but what reaches it is a general management toolkit; the I&C architecture being settled now, at the design stage, is addressed by neither track.

The relation to the other regimes has not been settled either. The investor is already an important entity under the national cybersecurity system; the operator will simultaneously be an essential entity under that system, the addressee of the ABW accreditation requirements under Article 36c(4) of the Atomic Law, and an entity overseen by the President of the PAA as regards physical protection and nuclear safety. Each of these regimes has its own authority, its own procedure for confirming conformity and its own reporting duties. The literature on the implementation of NIS 2 in the energy sector describes this type of regime overlap as a recurring problem [56], as do analyses of cybersecurity standards in the electricity sector [38, 39]. In the Polish setting, the relation between cybersecurity and the protection of critical infrastructure has already been the subject of legal analysis [55].

8. Coverage map and gaps

The juxtaposition in Figure 5 puts the above in order. I took the elements of the NSS 33-T methodology as the axis and checked whether, and where, each finds a counterpart in national law. I repeat the reservation from section 2: this is an expert judgement based on a reading of the texts, not a measurement.

Five elements have no counterpart in national law at all. There is no obligation to identify and inventory sensitive digital assets. There are no computer security levels as a normative category, and no computer security zones. There is no requirement to present a defensive computer security architecture as an element of the documentation. There are no rules for data flow between levels, including the one-way rule for connections with systems at the highest level.

Three elements are covered in part. Grading of requirements exists, but in its reliability version: § 85(2) of the design regulation ties the reliability level to the importance

	■ no counterpart	■ partial coverage	■ covered
Identification of sensitive digital assets	■	—	
Computer security levels	■	—	
Computer security zones	■	—	
Defensive security architecture	■	—	
Data flow rules between levels	■	—	
Grading of requirements by threat	■	§ 85(2) by consequence; § 20 of 2011 reg. — risk analysis	
System life cycle requirements	■	§§ 85, 90 — quality; § 18 of 2011 reg. for classified systems	
Protection against deliberate acts	■	§ 90(6) — a norm with no operational content	
Intentional threat in threat assessment	■	DBT lists cyber-attack; Art. 41n; NSS 10-G (Rev. 1)	
Security management	■	investor from 2026; operator from the operating licence	
Confidentiality, integrity, availability	■	Art. 36c(4) + 2011 reg. (§ 5); access control; ABW	

The author's expert assessment based on a reading of the legal texts. The compilation does not derive from measurement.

Fig. 5. Coverage of the elements of the NSS 33-T methodology [17] by Polish provisions — an expert assessment. The compilation does not derive from measurement; it is the author's judgement based on a reading of the texts of the legal acts and guidance.

of the safety function, which is grading by consequence, not by threat. Life cycle requirements are present and quite developed, except that they concern the quality of production, not resistance to attack; for the systems under Article 36c(4), § 18 of the 2011 regulation adds security duties spanning the system's whole period of operation [4]. Protection against intentional action exists as a norm, in § 90(6), but without operational content.

Three elements are covered in a way I consider sufficient at the statutory level. The inclusion of intentional threats in threat assessment is ensured by the definition of the design basis threat, which lists cyber-attack, and by Article 41n, with the methodology for a cyber-inclusive threat assessment supplied by NSS 10-G (Rev. 1) [22]. Security management on the organisational side is covered by the national cybersecurity regime: for the investor, as an important entity, already now, with the twelve-month implementation period of Article 33(1); for the operator, from the operating licence. Access control and the protection of confidentiality are covered by Article 36c(4) and the classified information regime, whose 2011 implementing regulation reaches beyond confidentiality to integrity, availability, risk management and security testing [4].

Four practical conclusions follow from this pattern.

First, the gap is largest where decisions are hardest to reverse. The elements not covered at all (assets, levels, zones, architecture and data flows) are settled in the design. The elements covered well (management, reporting, access control) can be introduced later. The distribution of the gaps is the inverse of the distribution of urgency.

Second, the shortest remedial path does not run through the statute. The delegation in Article 36c(3) of the Atomic Law directs the Council of Ministers to lay down the design requirements taking into account the recommendations of the IAEA and WENRA. The delegation concerning physical protection allows the content of the

protection system to be regulated. The design basis threat lists cyber-attack, and the President of the PAA draws it up. Introducing the concepts of computer security into the implementing regulations, or into regulatory guidance, sits within the existing authorisations.

Third, the regulator has a tool already. The construction licence application comes with safety analyses and documentation, and the President of the PAA approves the physical protection system and may attach conditions concerning the assurance of its effectiveness. Requiring the documentation to contain an identification of sensitive digital assets, an assignment of levels and a description of the defensive architecture calls for no new provision, only for that expectation to be stated in the proceedings. The Ukrainian regulator went down this road, working out a catalogue of computer security justification documents for I&C systems [35] and a methodology for assessing the computer security of those systems [42].

One more place deserves a note: the programme document itself. In the Polish Nuclear Power Programme the word “cybersecurity” occurs once, and not among the requirements for the facility, but in the list of fields of university study relevant to the nuclear programme [23]. The document that frames the whole undertaking treats cybersecurity as a staffing question, not a design question.

Fourth, Polish terminology is needed. The four load-bearing concepts of the IAEA methodology have no established Polish equivalents in normative texts. Until they exist, every set of documentation will translate them anew, and the regulator will be assessing things that go by different names. The Polish renderings proposed here (*wrażliwe aktywa cyfrowe, poziom bezpieczeństwa komputerowego, strefa bezpieczeństwa komputerowego, obronna architektura bezpieczeństwa komputerowego*) are offered as a starting point for discussion, not as a settlement.

9. Conclusions

Poland is building its first nuclear power plant at a moment when the international methodology for the computer security of I&C systems is mature and available. The IAEA has issued a complete set of guidance: NSS 42-G, NSS 17-T (Rev. 1) and NSS 33-T. The IEC has supplied a family of standards with a catalogue of controls. The material on which requirements can be based exists and is public.

The Polish legal order addresses this subject in four places, but it does so in four different languages. The design regulation speaks of reliability and mentions deliberate interference exactly once, although the IAEA warns in plain terms that safety analysis is not sufficient to define computer security requirements [20, para. 4.9]. The Atomic Law refers the systems supervising the process to the classified information regime, whose 2011 implementing regulation reaches beyond confidentiality to integrity, availability and risk management, with accreditation carried out by the ABW. The amended Act on the National Cybersecurity System, in force since 3 April 2026, covers the investor holding the principal decision as an important entity, with general duties enforceable within twelve months, and names the operator of a nuclear power facility as an essential entity only from the moment of obtaining the operating licence, roughly a decade away from the design decisions those obligations would be meant to secure. The physical protection regulation, still that of 2008, does not mention digital systems at all.

The national cybersecurity regime therefore reaches the investor already, but it operates with general management instruments alone and contains none of the I&C-specific concepts of the NSS 33-T methodology: sensitive digital assets, computer security levels, zones, the defensive architecture, the data flow rules. The other regimes do not introduce them either. Without them, design documentation and regulatory assessment lack a common language, and the grading of requirements remains grading by the consequence of failure, not by the intentional threat.

The conclusion is not alarmist, and it is not meant to be. The statutory framework contains everything needed to close these gaps: a definition of the design basis threat that lists cyber-attack, a delegation to lay down design requirements with an instruction to take IAEA recommendations into account, and the competence of the President of the PAA to approve the physical protection system and to set conditions for its effectiveness. What is missing are the implementing acts and the guidance that would translate the international methodology into the language of Polish regulatory practice. The moment for that is now, during the construction licence proceedings, not after them.

Limitations

This article relies on publicly available documents. I had no access to the design documentation of the Polish plant, or to internal regulatory guidance, if any has been produced. It is therefore possible that some of the identified gaps are being closed at the level of supervisory practice that is not public. The coverage assessment in Figure 5 is an expert judgement and open to debate. The analysis reflects the legal position as at 11 September 2026; given the pace of change in cybersecurity regulation and the ongoing revision of NSS 33-T, that position needs to be rechecked at every later use of this text. I did not analyse the United States requirements, which may carry practical significance given the choice of the AP1000 technology. That is a natural direction for further work.

Declarations

Funding: this work received no external funding.

Conflict of interest: the author declares no conflict of interest.

Statement on the use of artificial intelligence: No generative artificial intelligence tools were used in the preparation, drafting, editing, analysis, or review of this article. All content, analyses, conclusions, and figures were created by the author. The author personally verified all information presented in this work and bears full responsibility for its content. Artificial intelligence is not an author or co-author of this work.

Nature of the work: a review and conceptual article. It contains no original research, measurement data or experimental results.

About the author

Artur Chlebicki — MSc Eng. in Computer Science (Gdańsk University of Technology), independent researcher. Works professionally in the security of ICT systems. Areas of interest: security of industrial process control systems, cybersecurity regulation of critical infrastructure, assessment of the maturity of security processes. Contact: contact@chlebicki.art.

References

1. Legal acts (in chronological order)

1. Ustawa z dnia 29 listopada 2000 r. — Prawo atomowe (tekst jedn. Dz. U. z 2026 r. poz. 1).
2. Rozporządzenie Rady Ministrów z dnia 4 listopada 2008 r. w sprawie ochrony fizycznej materiałów jądrowych i obiektów jądrowych (Dz. U. Nr 207, poz. 1295).
3. Ustawa z dnia 29 czerwca 2011 r. o przygotowaniu i realizacji inwestycji w zakresie obiektów energetyki jądrowej oraz inwestycji towarzyszących (tekst jedn. Dz. U. z 2025 r. poz. 1156).
4. Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz. U. Nr 159, poz. 948).
5. Rozporządzenie Rady Ministrów z dnia 31 sierpnia 2012 r. w sprawie wymagań bezpieczeństwa jądrowego i ochrony radiologicznej, jakie ma uwzględniać projekt obiektu jądrowego (Dz. U. poz. 1048).

6. Rozporządzenie Rady Ministrów z dnia 11 lutego 2013 r. w sprawie wymagań dotyczących rozruchu i eksploatacji obiektów jądrowych (Dz. U. poz. 281).
7. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (tekst jedn. Dz. U. z 2026 r. poz. 20).
8. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii (Dz. Urz. UE L 333 z 27.12.2022, s. 80).
9. Ustawa z dnia 23 stycznia 2026 r. o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (Dz. U. poz. 252).

II. IAEA documents and technical standards (in chronological order)

10. INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Culture, IAEA Nuclear Security Series No. 7, IAEA, Vienna (2008).
11. INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5), IAEA Nuclear Security Series No. 13, IAEA, Vienna (2011).
12. INTERNATIONAL ATOMIC ENERGY AGENCY, Objective and Essential Elements of a State's Nuclear Security Regime, IAEA Nuclear Security Series No. 20, IAEA, Vienna (2013).
13. INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Nuclear Information, IAEA Nuclear Security Series No. 23-G, IAEA, Vienna (2015).
14. INTERNATIONAL ATOMIC ENERGY AGENCY, Design of Instrumentation and Control Systems for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-39, IAEA, Vienna (2016).
15. INTERNATIONAL ATOMIC ENERGY AGENCY, Leadership and Management for Safety, IAEA Safety Standards Series No. GSR Part 2, IAEA, Vienna (2016).
16. INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants — Instrumentation and Control Systems — Requirements for Coordinating Safety and Cybersecurity, IEC 62859:2016, IEC, Geneva (2016), with amendment IEC 62859:2016/AMD1:2019; consolidated version IEC 62859:2016+AMD1:2019 CSV (ed. 1.1), IEC, Geneva (2019).
17. INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security of Instrumentation and Control Systems at Nuclear Facilities, IAEA Nuclear Security Series No. 33-T, IAEA, Vienna (2018).
18. INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants — Instrumentation, Control and Electrical Power Systems — Cybersecurity Requirements, IEC 62645:2019, 2nd ed., IEC, Geneva (2019).
19. INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants — Instrumentation, Control and Electrical Power Systems — Security Controls, IEC 63096:2020, IEC, Geneva (2020).
20. INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security Techniques for Nuclear Facilities, IAEA Nuclear Security Series No. 17-T (Rev. 1), IAEA, Vienna (2021).
21. INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security for Nuclear Security, IAEA Nuclear Security Series No. 42-G, IAEA, Vienna (2021).
22. INTERNATIONAL ATOMIC ENERGY AGENCY, National Nuclear Security Threat Assessment, Design Basis Threats and Representative Threat Statements, IAEA Nuclear Security Series No. 10-G (Rev. 1), IAEA, Vienna (2021).
23. Program polskiej energetyki jądrowej — projekt aktualizacji z 2025 r. skierowany do konsultacji publicznych [Polish Nuclear Power Programme, draft 2025 update, public consultation version], Rada Ministrów, Warszawa (2025).
24. POLSKIE ELEKTROWNIE JĄDROWE sp. z o.o., Złożenie wniosku o wydanie zezwolenia na budowę obiektu jądrowego [Filing of the application for a licence to construct a nuclear facility], press release of 31 March 2026, Warszawa (2026).

IV. Secondary literature (in chronological order)

25. LANGNER, R., Stuxnet: Dissecting a Cyberwarfare Weapon, IEEE Security & Privacy 9 (2011) 49–51, doi: 10.1109/msp.2011.67.
26. PIGGIN, R., Development of industrial cyber security standards: IEC 62443 for SCADA and industrial control system security, IET Conference on Control and Automation, Birmingham (2013), doi: 10.1049/cp.2013.0001.
27. SEMA, P., ZAVARSKY, P., RUHL, R., A critical review of attack scenarios on the IAEA Technical Guidance NSS 17 Computer Security at Nuclear Facilities, World Congress on Internet Security (WorldCIS-2014), IEEE (2014) 87–90, doi: 10.1109/worldcis.2014.7028173.
28. KLEVTSOV, A., SYMONOV, A., TRUBCHANINOV, S., Computer Security of NPP Instrumentation and Control Systems: Categorization, Nuclear and Radiation Safety 4(72) (2016) 65–70, doi: 10.32918/nrs.2016.4(72).10.
29. HEALEY, A.N., The insider threat to nuclear safety and security, Security Journal 29 (2016) 23–38, doi: 10.1057/sj.2015.42.
30. LITHERLAND, P., ORR, R., PIGGIN, R., Cyber security of operational technology: understanding differences and achieving balance between nuclear safety and nuclear security, 11th International Conference on System Safety and Cyber-Security, IET (2016), doi: 10.1049/cp.2016.0856.
31. OECD NUCLEAR ENERGY AGENCY, Implementation of Defence in Depth at Nuclear Power Plants, OECD Publishing, Paris (2016), doi: 10.1787/9789264253001-en.
32. SYMONOV, A., KLEVTSOV, A., TRUBCHANINOV, S., Computer Security of NPP Instrumentation and Control Systems: Protective Measures against Computer Threats, Nuclear and Radiation Safety 2(74) (2017) 46–50, doi: 10.32918/nrs.2017.2(74).09.
33. BIAN, Y., LI, J., YIN, B., Analysis of Cyber Security Incident in South Korean Nuclear Power Plant and Cyber Security Solutions for Nuclear Power Industry, Proceedings of ICONE25, ASME (2017), doi: 10.1115/icone25-67577.
34. GURI, M., MONITZ, M., ELOVICI, Y., Bridging the Air Gap between Isolated Networks and Mobile Phones in a Practical Cyber-Attack, ACM Transactions on Intelligent Systems and Technology 8 (2017) 1–25, doi: 10.1145/2870641.
35. SYMONOV, A., KLEVTSOV, O., TRUBCHANINOV, S., LAZURENKO, O., Computer Security of NPP Instrumentation and Control Systems: Computer Security Justification Documents, Nuclear and Radiation Safety 4(84) (2019) 73–81, doi: 10.32918/nrs.2019.4(84).09.
36. ROBBINS, M., Cyberattack Hits Indian Nuclear Plant, Arms Control Today, December 2019.
37. JAKÓBIK, W., NOWAK, Z., NOWAKOWSKI, R., Energetyka jądrowa w Polsce [Nuclear power in Poland], Sprawy Międzynarodowe 72 (2019) 245–255, doi: 10.35757/sm.2019.72.3.08.
38. LESZCZYNA, R., Cybersecurity in the Electricity Sector, Springer, Cham (2019), doi: 10.1007/978-3-030-19538-0.
39. LESZCZYNA, R., Cybersecurity Standards Applicable to the Electricity Sector, in: Cybersecurity in the Electricity Sector, Springer, Cham (2019) 59–86, doi: 10.1007/978-3-030-19538-0_3.
40. KIM, S., HEO, G., ZIO, E., SHIN, J., Cyber attack taxonomy for digital environment in nuclear power plants, Nuclear Engineering and Technology 52 (2020) 995–1001, doi: 10.1016/j.net.2019.11.001.
41. PARK, J.W., LEE, S.J., A quantitative assessment framework for cyber-attack scenarios on nuclear power plants using relative difficulty and consequence, Annals of Nuclear Energy 142 (2020) 107432, doi: 10.1016/j.anucene.2020.107432.
42. KLEVTSOV, O., SYMONOV, A., TRUBCHANINOV, S., Computer Security of NPP Instrumentation and Control Systems: Computer Security Assessment, Nuclear and Radiation Safety 4(88) (2020) 69–76, doi: 10.32918/nrs.2020.4(88).09.

III. Programme documents

23. Program polskiej energetyki jądrowej — projekt aktualizacji z 2025 r. skierowany do konsultacji publicznych [Polish Nuclear Power Programme, draft 2025 update, public consultation version], Rada Ministrów, Warszawa (2025).

43. TRUBCHANINOV, S., International Standard Bases, in: *Cyber Security and Safety of Nuclear Power Plant Instrumentation and Control Systems*, IGI Global, Hershey (2020) 27–55, doi: 10.4018/978-1-7998-3277-5.ch002.
44. JOHNSON, G., Cyber Robust Systems, in: *Cyber Security and Safety of Nuclear Power Plant Instrumentation and Control Systems*, IGI Global, Hershey (2020) 163–174, doi: 10.4018/978-1-7998-3277-5.ch006.
45. BREZHNIEV, E., IVANCHENKO, O., NPP-Smart Grid Mutual Safety and Cyber Security Assurance, in: *Cyber Security and Safety of Nuclear Power Plant Instrumentation and Control Systems*, IGI Global, Hershey (2020) 349–380, doi: 10.4018/978-1-7998-3277-5.ch014.
46. ZHANG, F., COBLE, J.B., Robust localized cyber-attack detection for key equipment in nuclear power plants, *Progress in Nuclear Energy* 128 (2020) 103446, doi: 10.1016/j.pnucene.2020.103446.
47. XI, W., GU, P., LIU, W., Discussions on Information Security Test Strategy for Digital Industrial Control System in Nuclear Power Plant, *Lecture Notes in Electrical Engineering*, Springer, Singapore (2020) 83–89, doi: 10.1007/978-981-15-1876-8_9.
48. GARCIA, I., Nuclear Energy Agency's Consensus Position on the Impact of Cyber Security Features on Digital Instrumentation and Control Safety Systems, *NPIC&HMIT* 12 (2021) 1437–1444, doi: 10.13182/t124-34209.
49. STRUPCZEWSKI, A., Energetyka jądrowa koniecznym elementem elektroenergetyki polskiej [Nuclear power as a necessary element of the Polish electricity system], *ACADEMIA. Magazyn Polskiej Akademii Nauk* (2021) 88–97, doi: 10.24425/academiapan.2021.136854.
50. YANG, A., Discussion on Functional Safety and Cyber Security of I&C System in Nuclear Facilities, *Proceedings of ICONE29*, ASME (2022), doi: 10.1115/icone29-90807.
51. YANG, A., Research on Cyber Security Standards of Nuclear Power Industry Control System, *Lecture Notes in Electrical Engineering*, Springer, Singapore (2022) 75–84, doi: 10.1007/978-981-19-1181-1_8.
52. AGHARA, S., SPIRITO, C., Cyber Security for Nuclear Facilities, in: *The Oxford Handbook of Nuclear Security*, Oxford University Press, Oxford (2023) 309–324, doi: 10.1093/oxfordhb/9780192847935.013.29.
53. HUANG, Y., WANG, J., GU, H., ZHOU, X., False data injection attack detection for nuclear reactor based on chaotic time/frequency-hopping spread spectrum watermarking, *Process Safety and Environmental Protection* 176 (2023) 841–851, doi: 10.1016/j.psep.2023.06.068.
54. KHRIPUNOV, I., Nuclear Security Culture as a Tool to Address Insider Threat, in: *Advanced Sciences and Technologies for Security Applications*, Springer, Cham (2023) 115–126, doi: 10.1007/978-3-031-20278-0_8.
55. CZURYK, M., Cybersecurity and Protection of Critical Infrastructure, *Studia Iuridica Lublinensia* 32 (2023) 43–52, doi: 10.17951/sil.2023.32.5.43-52.
56. TEICHMANN, F., Cybersecurity of critical infrastructure in Europe: the NIS2 directive in focus, *International Cybersecurity Law Review* 6 (2025) 207–220, doi: 10.1365/s43439-025-00154-4.
57. JAATUN, M.G., LUNDTEIGEN, M.A., THIEME, C.A., FLÅ, L.H., Security Aspects of Zones and Conduits in IEC 62443, *Journal of Cybersecurity and Privacy* 6 (2026) 52, doi: 10.3390/jcp6020052.