Цивільна безпека

УДК 004.4 **doi: 10.26906/SUNZ.2023.2.170**

Б. Ю. Вінтенко[1], О. А. Смірнов[2], О. В. Коваленко[2], С. А. Смірнов[2], А. С. Коваленко[2]

[1] ПАТ "Науково-виробниче підприємство "Радій", Кропивницький, Україна
[2]Центральноукраїнський національний технічний університет, Кропивницький, Україна

ДОСЛІДЖЕННЯ НОРМАТИВНИХ ДОКУМЕНТІВ ТА ГАЛУЗЕВИХ СТАНДАРТІВ РОЗРОБКИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ КОМП'ЮТЕРНИХ СИСТЕМ УПРАВЛІННЯ АЕС, ВАЖЛИВИХ ДЛЯ БЕЗПЕКИ

Анотація. На сьогоднішній день одним з основних джерел електричної енергії є атомні електростанції (АЕС). В сучасному світі для управління технологічними процесами та забезпечення безпеки на АЕС використовуються цифрові системи управління з широким застосуванням комп'ютерів та контролерів. Від якості та надійності програмного забезпечення таких систем залежить безпечна експлуатація АЕС. В даній роботі проведено дослідження нормативних документів та стандартів, які мають відношення до розробки програмного забезпечення комп'ютерних систем управління АЕС, важливих для безпеки. **Метою** роботи є визначення стандартів, що можуть використовуватися розробниками програмного забезпечення для комп'ютерних систем управління АЕС, важливих для безпеки. **Об'єктом дослідження** є процес розробки програмного забезпечення для комп'ютерних систем управління АЕС. **Предметом** є дослідження нормативних документів та галузевих стандартів розробки програмного забезпечення для комп'ютерних систем управління АЕС. **У результаті дослідження** визначені критерії безпеки комп'ютерних систем управління, досліджено стандарти IEC 61508 та IEC 61513, досліджена настанова з безпеки МАГАТЕ SSG-39, визначені категорії функцій управління та класи безпеки систем АЕС, досліджені стандарти, що містять вимоги до програмного забезпечення, інтерфейсів користувача та кодування MISRA C/C++. **Висновки.** З метою створення високонадійного та якісного програмного забезпечення комп'ютерних систем керування АЕС, важливих для безпеки, в світі існують стандарти проектування та галузеві нормативні документи. Результатом дослідження стандартів та галузевих нормативних документів, які мають відношення до розробки програмного забезпечення комп'ютерних систем управління АЕС, важливих для безпеки є наступне: міжнародні стандарти та нормативні документи мають різні рівні спеціалізації. В документах вищого рівня наводяться загальні вимоги до всіх етапів життєвого циклу комп'ютерних систем управління та містяться посилання на документи наступного рівня. Документи наступного рівня є більш спеціалізованими і мають відношення до більш вузьких сфер діяльності; кожна країна світу може визначати свій набір стандартів та нормативних документів, який вимагається використовувати під час проектування та реалізації комп'ютерних систем управління для АЕС; в нормативних документах містяться вимоги та рекомендації як щодо організації процесу розробки, так і загальні рекомендації та приклади написання коду програм різними мовами програмування; через те, що вимоги розглянутих стандартів мають бути актуальними протягом тривалого часу, ці стандарти не містять формалізованих методик написання коду програм; не існує формалізованих методик сертифікації коду на відповідність вимог розглянутих стандартів; кожна організація, яка займається проектуванням, розробкою та верифікацією програмного забезпечення комп'ютерних систем управління для АЕС, повинна розробити власні методики з застосування вимог та оцінки критеріїв виконання вимог стандартів та нормативів. Таким чином, зроблено висновок, що перспективами подальших досліджень є детальний аналіз вимог міжнародних стандартів та галузевих нормативних документів до програмного забезпечення комп'ютерних систем управління АЕС та розробка методики його написання й оцінки відповідності вимогам стандартів.

Ключові слова: програмне забезпечення, комп'ютерні системи управління, АЕС.

Вступ

Постановка проблеми. На сьогоднішній день одним з основних джерел електричної енергії є атомні електростанції (АЕС). В багатьох країнах світу, зокрема в Словаччині, Франції, Україні [1] обсяги атомної генерації становлять понад 50%. Використання атомної енергії є екологічно чистим та економічно вигідним, проте має високі вимоги до безпеки та надійності для забезпечення захисту людини та навколишнього середовища від радіаційного випромінювання ядерного палива. В сучасному світі для управління технологічними процесами та забезпечення безпеки на АЕС використовуються цифрові системи управління з широким застосуванням комп'ютерів та контролерів. Від якості та надійності програмного забезпечення (ПЗ) таких систем залежить безпечна експлуатація АЕС.

Аналіз останніх досліджень і публікацій. Цифрові системи управління потребують особливих підходів до розробки та оцінювання надійності в порівнянні з аналоговими системами, оскільки в силу свого характеру та призначення допускають більшу свободу під час проектування [11]. Ці підходи мають відповідати визначеним вимогам. Вимоги до підходів проектування, реалізації, верифікації, валідації та інших етапів життєвого циклу таких систем описуються в міжнародних стандартах [2, 3], публікаціях МАГАТЕ [11] та галузевих нормативних документах різних країн [16–19].

Ці документи є обов'язковими для використання всіма учасниками процесів проектування, розробки, впровадження та експлуатації комп'ютерних систем управління (КСУ).

Дослідження вимог стандартів проектування та розробки КСУ проведено в роботах [20–23]. Детальні

вимоги до ПЗ КСУ АЕС описуються в міжнародних стандартах [5, 6], а також, наприклад, в галузевому стандарті США [7]. Вимоги до інтерфейсів користувача КСУ АЕС описуються в міжнародних стандар-тах [7, 8], а також, наприклад, в галузевому стандарті США [14]. Схема взаємозв'язків міжнародних та галузевих стандартів, на які посилається дана робота, показана на рис. 1.

Постановка задач дослідження

В даній роботі необхідно провести дослідження нормативних документів та стандартів, які мають відношення до розробки програмного забезпечення КСУ АЕС, важливих для безпеки. **Метою** роботи є визначення стандартів, що можуть використовуватися розробниками програмного забезпечення для КСУ АЕС, важливих для безпеки. **Об'єктом дослідження** є процес розробки програмного забезпечення для КСУ АЕС. **Предметом** є дослідження нормативних документів та галузевих стандартів розробки програмного забезпечення для КСУ АЕС.

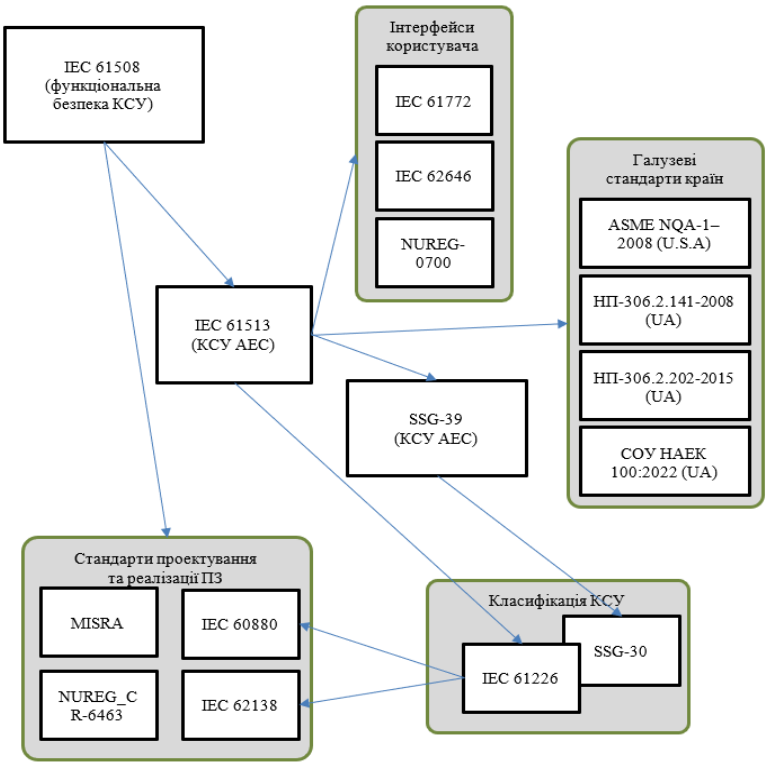

Рис. 1. Схема взаємозв'язків міжнародних та галузевих стандартів

Безпека комп'ютерних систем управління

Комп'ютерні системи управління (КСУ) згідно з стандартом IEC 61508 є окремим випадком систем контролю та управління (СКУ). СКУ – це система, що приймає вхідні сигнали від процесу (датчиків) та/або оператора, обробляє вхідні параметри згідно з необхідними технологічними алгоритмами та генерує вихідні сигнали, зумовлюючи роботу керованого об'єкту необхідним чином. СКУ, що базуються на КСУ все в більших об'ємах використовуються для виконання функцій безпеки на об'єктах, які можуть створювати ризики для людей та навколишнього середовища (атомні електростанції, газова та нафтова промисловість, транспорт, хімічне виробництво). СКУ на таких об'єктах мають відповідати певним характеристикам безпеки (резервування, самодіагностика, стійкість до відмов). КСУ мають високий рівень програмної складової, для якої існують, зокрема, вимоги інформаційної безпеки (Security Requirements) [20]. Згідно з ними, дані та програмне забезпечення мають бути захищеними від несанкціонованого доступу та несанкціонованих змін. Інформаційна безпека описана в групі стандарті ISO/IEC 27000 [9], нормативному документі NIST SP 800-82 «Guide to Industrial Control Systems (ICS) Security» [10]. Разом з тим, для КСУ важливими є вимоги функціональної безпеки (Safety Requirements). Функціональна безпека системи забезпечує коректність виконання функцій управління об'єктом, у випадку відмови системи – переведення об'єкту керування в безпечний стан. Її вимоги стосуються не тільки програмної складової, а і апаратного забезпечення, електричного та електронного обладнання та механічних пристроїв, а також власне інформаційної безпеки [20].

Загальні стандарти функціональної безпеки для КСУ наведено в міжнародних стандартах, таких як IEC 61508 [2].

Стандарт з функціональної безпеки КСУ IEC 61508

Стандарт IEC 61508 « Functional safety of electrical/electronic/programmable electronic safety-related systems» [2] є стандартом верхнього рівня для функціональної безпеки (ФБ) КСУ. Виконання вимог цього стандарту підвищує надійність та життєздатність продукту, а також формалізує та систематизує процеси проектування, розробки, тестування та впровадження. Стандарт IEC 61508 складається з семи частин. Частина IEC 61508-1 описує загальні вимоги до функціональної безпеки, частина IEC 61508-2 –додаткові вимоги до апаратних засобів, частина IEC 61508-3 – додаткові вимоги до програмного забезпечення та документації, частина IEC 61508-4 містить терміни та визначення. Інші частини мають довідковий характер. Частина стандарту IEC 61508-1 визначає вимоги до керування функціональною безпекою та вимоги до життєвого циклу (ЖЦ) системи в контексті промислового об'єкту автоматизації. Вона визначає такі етапи ЖЦ як концепція, розробка, верифікація, валідація, впровадження, експлуатація, супроводження, зняття з експлуатації.

В частині стандарту IEC 61508-2 додаються вимоги до апаратної складової КСУ. Проте ця частина містить додатки, які мають враховувати і розробники програмного забезпечення. Додатки А та В описують підхід до реалізації самодіагностики та захисту від одиничних відмов. Додаток С містить рекомендації з розрахунку діагностичного покриття з метою забезпечення потрібного рівня повноти безпеки (Safety

Integrity Level, SIL). Додаток D містить вимоги до керівництва з експлуатації з урахуванням вимог безпеки (Safety Manual).

Частина стандарту IEC 61508-3 конкретизує вимоги до програмного забезпечення КСУ. Зокрема, розділ 7 наводить деталізовані вимоги до життєвого циклу ПЗ.

У підрозділі 7.1 наводиться підхід до розділення процесу розробки програмного забезпечення на етапи, описані в підрозділах 7.2-7.9 стандарту.

Підрозділ 7.2 містить вимоги щодо етапу специфікації вимог до функцій безпеки програмного забезпечення та стійкості до систематичних відмов. Специфікація вимог має враховувати самоконтроль ПЗ, моніторинг апаратного забезпечення, періодичне тестування функцій безпеки тощо.

Підрозділи 7.3 та 7.7 наводять вимоги до етапу планування та виконання процедур підтвердження відповідності аспектів програмного забезпечення до вимог безпеки системи.

Підрозділ 7.4 містить загальні вимоги до етапу проектування та розробки програмного забезпечення. Це вимоги:

– до проектування архітектури програмного забезпечення;

– до вибору інструментальних засобів розробки;

– до реалізації ПЗ з урахуванням вимог специфікації;

– до підходів тестування програмних модулів.

Підрозділ 7.5 описує підходи до етапу інтеграції програмного забезпечення та апаратних засобів. Метою вимог цього підрозділу є об'єднання ПЗ та апаратних засобів та перевірка їх відповідності вимогам повноти безпеки.

Підрозділ 7.6 описує процедури етапів експлуатації та модифікації програмного забезпечення. Мета цих процедур – впевнитися в тому, що функціональна безпека системи зберігається під час експлуатації та модифікації.

Підрозділ 7.8 детально описує процедури модифікації програмного забезпечення.

Підрозділ 7.9 детально описує процедури верифікації програмного забезпечення.

В додатку А стандарту IEC 61508-3 приведена настанова з вибору методів та засобів проектування програмного забезпечення. В додатку В стандарту IEC 61508-3 приведені детальні вимоги до методів та засобів проектування.

Дослідження стандарту IEC 61508 **дозволяє зробити висновок**, що він містить важливі вимоги до всіх етапів життєвого циклу програмного забезпечення КСУ. Згідно стандарту IEC 61508 застосування багатьох підходів, залежить від конкретних практик, засобів та мов програмування, що використовуються, але на більшості рівнів повноти безпеки (SIL) можна виділити загальні підходи до розробки ПЗ:

– використання сертифікованих інструментальних засобів;

– використання перевірених елементів ПЗ (за їх наявності);

– застосування модульності та структурного програмування;

– використання стандартів кодування (наприклад, MISRA C/C++);

– застосування формальних та напівформальних методів розробки та тестування;

– застосування засобів діагностування;

– статичний аналіз коду;

– контроль часових характеристик виконання програми;

– верифікація ПЗ.

Особливість верифікації програмного коду модулів полягає в аналізі критичності ПЗ, при якому встановлюється ступінь критичності модулів для виконання функцій безпеки. Це дозволяє знизити об'єм заходів для другорядного ПЗ та сконцентруватися на найбільш відповідальному ПЗ.

Наступний етап включає в себе дослідження стандартів розробки ПЗ, що мають безпосереднє відношення до атомних станцій.

Стандарт IEC 61513. Проектування КСУ АЕС, важливих для безпеки

Вимоги стандарту IEC 61508 [2] не є спеціалізованими виключно для атомної галузі. Для різних областей діяльності вимоги стандарту деталізовані в інших стандартах, наприклад IEC 61511 – для небезпечних виробництв, IEC 62061 – для машинобудування. Стандарт **IEC 61513** «Nuclear power plants – Instrumentation and control important to safety – General requirements for systems» [3] є головним в ієрархії стандартів для КСУ, важливих для безпеки атомних станцій. Він встановлює загальні вимоги для архітектури та обладнання КСУ АЕС, важливих для безпеки, що створюються на основі як аналогових, так і цифрових технологій. В багатьох країнах вимагається сертифікація КСУ атомних станцій згідно з стандартами IEC 61508/IEC 61513.

Загальна модель життєвого циклу КСУ АЕС, що приводиться в стандарті IEC 61513, запозичена з стандарту IEC 61508. Стандарт IEC 61513 забезпечує інтерпретацію частин IEC 61508-1, IEC 61508-2, IEC 61508-4 до ядерної галузі. Вимоги частини IEC 61508-3, що стосуються програмного забезпечення КСУ АЕС ВБ, інтерпретуються в стандартах IEC 60880 [5] та IEC 61238 [6]. Розділ 5 стандарту IEC 61513 присвячено загальній структурі життєвого циклу комп'ютерних систем управління АЕС, важливих для безпеки. Він містить вимоги до наступних етапів та процесів проектування КСУ АЕС:

– визначення функцій контролю та управління АЕС (підрозділ 5.2.2);

– категоризацію функцій контролю та управління АЕС в залежності від впливу на безпеку (підрозділ 5.2.3);

– аналізу обмежень проекту конкретної АЕС (підрозділ 5.2.4);

– декомпозицію загальної архітектури КСУ з розподіленням її на окремі підсистеми (підрозділ 5.4.2);

– визначення функцій та інтерфейсів підсистем КСУ (підрозділ 5.4.3);

– планування забезпечення якості КСУ (підрозділ 5.5.2);

– планування захищеності КСУ(підрозділ 5.5.3);

– планування загальної інтеграції КСУ та вводу її в експлуатацію (підрозділ 5.5.4).

В результаті виконання має бути розроблена вихідна документація з проекту архітектури КСУ та функцій, які будуть виконуватися (підрозділ 5.6).

В розділі 6 стандарту IEC 61513 наводяться вимоги до етапів життєвого циклу окремих підсистем КСУ. Перелік етапів включає в себе такі пункти:

– специфікація вимог до функцій підсистеми, обмежень, інтерфейсів користувача, умов навколишнього середовища;

– специфікація системи, аналіз існуючого обладнання, розробка проекту архітектури підсистеми, призначення прикладних функцій;

– детальне проектування та реалізація апаратних засобів та програмного забезпечення, валідація вимог до прикладних функцій;

– інтеграція компонентів програмного та апаратного забезпечення в єдину систему;

– валідація системи;

– монтаж та випробовування системи;

– планування подальшої валідації, експлуатації та модифікації.

Розділи 7 та 8 містять вимоги до процесів загальної інтеграції, експлуатації та технічного обслуговування системи.

Аналіз вимог стандарту IEC 61513 **дозволяє зробити висновок**, що він не містить прямих вимог до особливостей розробки програмного забезпечення. Проте він визначає процеси, в яких беруть участь розробники програмного забезпечення. Також він вказує на стандарт, що визначає класифікацію КСУ АЕС з функціональної безпеки [4], а також на стандарти, що містять конкретні вимоги до програмного забезпечення в залежності від класу функціональної безпеки [5, 6]. Посилання на стандарт IEC 61513 містяться в різних нормативних документах з безпеки КСУ АЕС. Це публікації міжнародних організацій [11], а також галузеві стандарти різних країн [16–19].

Настанова з безпеки МАГАТЕ SSG-39

Настанова з безпеки МАГАТЕ **SSG-39** «Design of Instrumentation and Control Systems for Nuclear Power Plants, Specific Safety Guide No. 39» [11] є публікацією, що спирається на стандарт IEC 61513 та відповідає його вимогам. Цей документ також містить рекомендації щодо всіх етапів розробки КСУ АЕС, важливих для безпеки.

Розділ 2 присвячений менеджменту проектування КСУ. Він містить опис всіх етапів життєвого циклу КСУ. В розділі 3 описуються методи визначення функцій контролю та керування АЕС. Розділ 4 містить рекомендації щодо проектування загальної архітектури КСУ та розділення системи керування та контролю на окремі функціональні підсистеми. Розділ 5 описує класифікацію функцій та систем безпеки.

Розділ 6 містить загальні вимоги до систем, важливих для безпеки. Сюди входять пункти щодо надійного проектування, захищеності, випробувань, здатності до ремонту, технічного обслуговування, маркування тощо.

Розділ 7 описує принципи проектування конкретних систем.

Розділ 8 містить вимоги до інтерфейсу «людина»-«машина».

Розділ 9 містить вимоги щодо програмного забезпечення КСУ. Це загальні вимоги до програмного забезпечення (пункти 9.6-9.15), вимоги до його проектування (пункти 9.16-9.43), реалізації (пункти 9.44-9.66), верифікації (пункти 9.64-9.95). В пунктах 9.96-9.98 містяться вимоги до застосування раніше розробленого ПЗ.

В результаті дослідження публікації **МАГАТЕ SSG-39 можна зробити висновок**, що цей документ містить важливі вимоги до менеджменту розробки, проектування, апаратного та програмного забезпечення КСУ. Він містить посилання на інші відповідні міжнародні стандарти, що дає можливість проектантам КСУ підібрати необхідні для вивчення документи.

Категорії функцій управління та класи безпеки систем АЕС

Функції систем контролю та управління АЕС класифікуються в категорії, що означають важливість функції для безпеки. Важливість функції для безпеки оцінюється наслідками її відмови тоді, коли необхідне її виконання, та наслідками хибного спрацювання (пункт 5.1 [4], пункт 3.15 [12]).

Методи класифікації систем на категорії безпеки встановлені в стандарті **IEC 61226** (Nuclear power plants – Instrumentation and control important to safety – Classification of instrumentation and control functions) [4], на який прямо посилається стандарт IEC 61513. Стандарт IEC 61226 застосовується для всіх інформаційних та управляючих функцій, а також систем, що реалізують ці функції. Згідно з пунктом 5.3 стандарту IEC 61226, існують три категорії функцій КСУ за важливістю для безпеки – «А», «В» та «С».

Методика розподілення систем на класи безпеки також міститься в документах МАГАТЕ **SSG-30** «Safety Classification of Structures, Systems and Components in Nuclear Power Plants» [12] та **TECDOC-1787** «Application of the Safety Classification of Structures, Systems and Components in Nuclear Power Plants» [13]. Розділ 3.16 [12] описує категорії безпеки 1, 2 та 3 в залежності їх впливу на безпеку. Згідно розділу 3.2.7 [13], для КСУ АЕС ці категорії відповідають категоріям «А», «В», «С» стандарту IEC 61226.

Категорія «А» (клас 1) використовується для систем, що грають основну роль в забезпеченні безпеки АЕС і відмова яких може безпосередньо привести до аварійних умов.

Категорію «В» (клас 2) мають системи, що грають додаткову роль в забезпеченні безпечних умов, зокрема у випадку, коли робота функцій цих систем виключить необхідність спрацювання функцій категорії «А». До цієї категорії також відносяться функції, відмова або хибне спрацювання яких може викликати або підсилити аварійний стан. Через наявність ешелону функцій безпеки категорії «А» вимоги до безпеки систем категорії «В» можуть бути не такими строгими, і функціональність таких систем може бути розширеною.

До категорії «С» (клас 3) відносять функції, що грають додаткову чи допоміжну роль. Вони мають відношення до забезпечення безпеки АЕС, але можуть безпосередньо не використовуватися для реагування на аварійні ситуації.

В свою чергу, нормативний документ **НП 306.2.141-2008 «Загальні положення безпеки атомних станцій»** [17], що діє в Україні, поділяє елементи АЕС на чотири класи безпеки. Клас 1 – це тепловиділяючі елементи (твели) та інші елементи, відмова яких є вихідними подіями, що призводять до пошкоджень тепловиділяючих елементів з перевищенням встановлених для проектних аварій меж. Клас 2 – елементи, відмова яких є вихідними подіями, що призводять до пошкоджень тепловиділяючих елементів в межах, встановлених для проектних аварій, а також елементи систем безпеки, відмови яких призводять до невиконання цими системами своїх функцій. Клас 3 – це елементи систем, важливих для безпеки, що не увійшли до класів 1 та 2. Клас 4 – це елементи систем нормальної експлуатації АЕС. Також для класів використовуються кваліфікаційні позначення літерою, що означають призначення елемента: Н – нормальна експлуатація, У – управляючі системи, Л – локалізуючі системи безпеки, З – захисні системи.

Нормативний документ України **НП 306.2.202-2015 «Вимоги з ядерної та радіаційної безпеки до інформаційних та керуючих систем, важливих для безпеки атомних станцій»** [18] та стандарт державного підприємства «НАЕК «Енергоатом» **СОУ НАЕК 100:2022 «Інформаційні та керуючі системи, важливі для безпеки атомних електричних станцій. Загальні технічні вимоги»** [19] аналогічно до стандарту IEC 61226 поділяють функції КСУ класів безпеки 2 та 3 за **НП 306.2.141-2008** на категорії «А», «В» та «С» залежно від їх ролі в забезпеченні та підтримці безпеки, а також можливим невиконанням або помилковим виконанням своїх функцій.

Класи безпеки систем АЕС за стандартом IEC 61513. Крім визначення категорій за функціями безпеки, стандарт IEC 61513 відносить КСУ, важливі для безпеки, до одного з трьох класів безпеки (додаток В. 4). Вимоги до функції безпеки найвищої категорії визначають клас безпеки системи. Так, до класу 1 відносяться системи аварійного електропостачання та активації захисту, а до класів 2 та 3 – системи автоматизації та контролю АЕС.

В результаті дослідження стандартів з класифікації систем та стандартів з функціональної безпеки **можна зробити висновок**, існує декілька градацій розділення КСУ за класами безпеки та категоріями впливу на безпеку. Вимоги до проектування та розробки програмного забезпечення можуть відрізнятися залежно від класу безпеки КСУ. Подальше дослідження буде стосуватися стандартів, що містять вимоги до програмного забезпечення з урахуванням категорії функцій безпеки.

Стандарти, що містять вимоги до програмного забезпечення

Стандарти IEC 61508, IEC 61513 не містять визначених вимог до програмного забезпечення КСУ АЕС, важливих для безпеки. Проте у вступі до стандарту IEC 61513, а також таблиці 1 пункту 7.1 стандарту IEC 61226 наведені посилання на інші стандарти, в яких ці вимоги вводяться. Для ПЗ систем категорії функцій безпеки «А» використовується стандарт IEC 60880, для систем категорій функцій безпеки «В», «С» – IEC 62138. Ці стандарти відповідають загальним вимогам стандарту IEC 61508-3 до програмного забезпечення КСУ в ядерній сфері.

Вимоги до програмного забезпечення КСУ, що виконують функції безпеки категорії «А», містяться в стандарті IEC 60880 «Nuclear power plants – Instrumentation and control systems important to safety – Software aspects for computer-based systems performing category A functions» [5]. Вимоги стандарту застосовуються до програмного забезпечення, що використовуються в КСУ АЕС для виконання функцій безпеки категорії «А». Це ПЗ, яке використовується для функцій захисту, а також запобігання розвитку проектних аварій і приведення станції в безпечний контрольований стан під час аварійних ситуацій, має бути створене з високим ступенем якості та надійності, пройти повний цикл верифікації та атестації. Мета вимог стандарту IEC 60880 – розробка ПЗ, що відповідає критеріям якості та надійності. Вимоги стандарту відносяться до всіх етапів життєвого циклу програмного забезпечення, включаючи специфікацію вимог, проектування, вибір інструментальних засобів та мов, розробку, верифікацію, валідацію, модифікацію тощо.

Розділ 3 стандарту IEC 60880 описує терміни та визначення. Зокрема, вводяться поняття універсальної мови програмування, проблемно-орієнтованої мови програмування, системного та прикладного програмного забезпечення, прикладної функції, стиснення коду, різноманітності, резервування, стійкості до дефектів та помилок тощо.

Розділ 4 містить список скорочень та позначень.

Розділ 5 містить загальні вимоги до проектам програмного забезпечення. В розділі розглядаються наступні концепції:

– життєвого циклу безпеки ПЗ в додаток до загального життєвого циклу системи керування;

– розподілу ПЗ та конфігураційних даних за типами (системне або прикладне);

– наявності підходів до розробки ПЗ за допомогою універсальних або проблемно-орієнтованих мов програмування;

– керування проектуванням ПЗ;

– керування забезпеченням якості ПЗ;

– захищеності ПЗ.

Розділ 6 присвячений етапу створення специфікації вимог до програмного забезпечення. Вимоги до ПЗ мають визначатися вимогами до системи безпеки і являтися частиною специфікації КСУ. Вони мають описувати те, що повинна робити програма, а не те, як вона повинна це робити. До основних вимог до ПЗ , що входять до специфікації, входять:

– чіткий опис прикладних функцій ПЗ, його поведінки, інтерфейсів користувача, часу відгуку, зв’язків з іншими системами, функціональних обмежень;

– наявність самоконтролю та збору діагностичної інформації;

– передбачення періодичних тестувань функцій безпеки;

– наявність чіткої документації.

Розділ 7 містить вимоги щодо проектування та реалізації програмного забезпечення.

В підрозділі 7.1 описані загальні принципи проектування та реалізації ПЗ. Наведені окремі вимоги до реалізації ПЗ з використанням універсальних та проблемно-орієнтованих мов програмування. Також наводяться вимоги до конфігурування раніше розробленого програмного забезпечення.

В підрозділі 7.2 наведені детальні вимоги щодо вибору мови програмування та інструментальних засобів.

Підрозділ 7.3 містить посилання на додаток В, що містить детальні вимоги і рекомендації з розробки ПЗ. Зазначається, що в процесі розробки ці вимоги та рекомендації мають виконуватися, а їх невиконання має бути документально обґрунтованим.

Розділ 8 визначає вимоги до верифікації ПЗ. В ньому наводяться окремі вимоги до планування процесу верифікації, верифікації проекту та його реалізації.

У розділі 9 знаходиться опис вимог до процесів інтеграції ПЗ до технічного забезпечення та його верифікації під час інтеграції.

Розділ 10 містить опис аспектів валідації ПЗ в складі інтегрованої системи. Має бути створений план валідації, який буде виконуватися особами, які не брали участь в проектуванні та реалізації системи. Для кожної функції має бути проведено комплексне всебічне тестування. За результатами тестувань мають бути складені звіти та визначені процедури усунення виявлених дефектів.

Розділ 11 описує вимоги до процесу модифікації ПЗ. Розглядаються вимоги до процедури запиту на модифікацію та процедури виконання модифікації.

Розділ 12 формує вимоги до установки та експлуатації ПЗ, його захищеності на місці експлуатації та навчання операторів.

Розділ 13 містить вимоги до захисту від дефектів ПЗ, що можуть призвести до відмови з загальної причини. Розглядаються підходи до проектування ПЗ з врахуванням критерію одиничної відмови, реалізація різноманітності.

Розділ 14 містить детальні вимоги до вибору, атестації та конфігурації інструментальних програм.

Стандарт IEC 60880 також містить додатки, які деталізують інформацію, наведену в розділах. За об'ємом вони займають половину розміру всього документу стандарту і є обов'язковими доповненнями до відповідних розділів. Зокрема:

– розділ А (обов'язковий) містить детальну інформацію щодо життєвого циклу ПЗ та формування вимог до ПЗ;

– розділ В (обов'язковий) містить деталізовані вимоги та рекомендації щодо процесу проектування ПЗ, структури ПЗ, самоконтролю, детального проектування та кодування;

– розділ С (довідковий) містить приклади технологій прикладного програмування;

– розділ D (довідковий) містить детальні вимоги до мов програмування та інструментальних засобів;

– інші розділи є також довідковими.

В результаті дослідження стандарту IEC 60880 **можна зробити висновок**, що він є одним з основних стандартів з розробки та проектування ПЗ КСУ АЕС, важливих для безпеки. Незалежно від технологій та мов програмування, що використовуються, розробники програмного забезпечення мають детально знати та чітко дотримуватись його рекомендацій.

Незважаючи на те, що вимоги цього стандарту відносяться до ПЗ категорії функціональної безпеки «А», вони можуть застосовуватися і при розробці ПЗ нижчих функціональних категорій. Це дозволить покращити якість та надійність ПЗ загалом, а також розширити межі використання розробленого програмного забезпечення до вищої категорії «А».

Стандарт не містить детальних методик досягнення та оцінки відповідності програмного коду своїм вимогам. **Тому в перспективі подальшого дослідження** цього стандарту є детальний аналіз вимог та створення методів написання та оцінки програмного коду.

Вимоги до програмного забезпечення КСУ, що виконують функції безпеки категорій «В» та «С», містяться в стандарті IEC 62138 «Nuclear power plants – Instrumentation and control important for safety – Software aspects for computer- based systems performing category B or C functions» [6]**.** Цей стандарт доповнює стандарт IEC 60880, який містить вимоги до програмного забезпечення КСУ, що виконує функції безпеки категорії «А». Також він доповнює загальний стандарт з функціональної безпеки КСУ АЕС IEC 61513 в об'ємі вимог до програмного забезпечення.

Мета даного стандарту – максимально знизити імовірність прихованих програмних дефектів, що можуть привести до системних відмов через одиничні або множинні програмні відмови (тобто відмови з загальної причини).

Вимоги стандарту IEC 62138 прив'язані не до категорій функцій безпеки, а до класу безпеки КСУ (клас 2 та клас 3 за стандартом IEC 61513), оскільки КСУ можуть одночасно реалізовувати як функції безпеки категорій «В», «С», так і не класифіковані за безпекою,

Розділ 3 стандарту IEC 62138 описує терміни та визначення.

Розділ 4 містить список скорочень та позначень.

Розділ 5 містить загальні концепції та положення. В ньому виділяються типи програмного забезпечення в залежності від типу робіт, що виконуються ним (системне та прикладне). Розглядаються типи конфігураційних даних. Наводиться архітектура життєвого циклу програмного забезпечення. Вводяться принципи градації вимог до програмного забезпечення в залежності від класу безпеки КСУ (класи безпеки 2 та 3 за IEC 61513 відповідно до категорії функцій безпеки «В» та «С»).

Розділ 6 містить вимоги до програмного забезпечення КСУ класів безпеки 2 та 3. В підрозділі 6.1 зазначається, що частина вимог цього розділу

застосовується до ПЗ обох класів безпеки, а окремі вимоги стосуються тільки ПЗ класу 2 або класу 3.

Підрозділ 6.2 містить загальні вимоги до життєвого циклу ПЗ та змісту програми контролю його якості. Зазначається, що кожний етап життєвого циклу ПЗ має включати дії, які необхідні для досягнення необхідної якості, а також дії з верифікації показників досягнення цієї якості. Мають бути заплановані заходи щодо керування конфігурацією та контролю версій ПЗ. Також наводяться загальні рекомендації щодо вибору інструментальних засобів та мов програмування.

Підрозділ 6.3 містить вимоги до вибору та аналізу раніше розробленого програмного забезпечення. Вимагається наявність документації з безпеки, докази коректності та функціональної відповідності цього ПЗ вимогам КСУ, що розробляється.

Підрозділ 6.4 доповнює та уточнює вимоги стандарту IEC 61513 про те, що вимоги до ПЗ повинні бути оформлені документально і сформована специфікація вимог до ПЗ. Вводяться вимоги до початкової інформації, згідно з якою створюється КСУ, та змісту специфікації ПЗ (наявність опису прикладних функцій, режимів роботи, інтерфейсів, обмежень тощо).

Підрозділи 6.5 та 6.6 стандарту IEC 61238 містять детальні вимоги до етапу проектування, початкових даних та етапу реалізації нового програмного забезпечення. Ці підрозділи не містять конкретних вимог щодо написання специфікації та коду програм, але містять інформацію, яким чином має виконуватися проектування та реалізація в залежності від класу безпеки системи. Розглянуті вимоги як для проблемно-орієнтованих, так і універсальних мов програмування.

Подальші підрозділи (6.7-6.11) містять вимоги до процесів інтеграції програмного та апаратного забезпечення, проведення процедур валідації системи, встановлення та експлуатацію програмного забезпечення на місці експлуатації та подальші модифікації. В підрозділі 6.12 вказується на необхідність з захисту КСУ від відмов з загальної причини внаслідок роботи програмного забезпечення та міститься посилання на стандарт IEC 61513, де це питання розглянуто більш детально. Додатки до стандарту є довідковою інформацією та не містять вимог до програмного забезпечення.

З дослідження стандарту IEC 61238 **можна зробити висновок**, що вимоги до реалізації ПЗ функцій безпеки категорій «B» та «C» є менш формальними та суворими, ніж ПЗ функцій безпеки до категорії «A», а є більш узагальнюючими. Проте в перспективі подальших досліджень для цих вимог є більш детальний їх аналіз з метою розробки методики написання ПЗ та оцінки його відповідності вимогам стандарту IEC 61238.

Стандарти інтерфейсів користувача

Інтерфейс користувача визначає зручність взаємодії людини з програмним забезпеченням. При створенні програмного забезпечення КСУ АЕС його інтерфейс користувача має забезпечувати безпомилковість, ефективність та зручність роботи операторів.

Зокрема, в **стандарті IEC 61772** «Nuclear power plants – Control rooms – Application of visual display units (VDUs)» [7] наводяться вимоги до пристроїв візуального відображення, які використовуються операторами АЕС. Ці вимоги мають бути враховані під час реалізації інтерфейсів користувача програмного забезпечення. Вони стосуються наступних аспектів:

– відбір інформації, яка має відображається;

– компонування та розміщення інформації;

– формат, розмір та колір елементів відображення;

– форма відображення інформації: алфавітно-цифрова, образна та символьна;

– забезпечення зручного вибору оператором інформації, необхідної на поточний момент.

Інший **стандарт IEC 62646** «Nuclear power plants – Control rooms – Computer-based procedures» [8] містить узагальнені вимоги до процедур керування АЕС, в яких застосовуються комп'ютери. Зокрема, згідно з цими вимогами, при проектуванні програмного забезпечення КСУ АЕС мають бути реалізовані:

– зручний інтерфейс «людина-машина»;

– чітка навігація між видами інформації;

– автоматизація процедур, що виконуються оператором;

– допомога оператору під час прийняття рішень.

Галузевий нормативний **документ NUREG-0700** «Human-System Interface Design Review Guidelines» розглядає інтерфейси користувачів КСУ з декількох напрямків.

В першій частині (розділи 1-3) розглядаються загальні вимоги до відображення інформації:

– до форматів відображення даних: (написи, списки, таблиці, гістограми, графіки, діаграми тощо);

– до елементів інтерфейсу користувача: символи, мітки, іконки, шкали, стрілки, кольорові схеми тощо;

– до швидкості оновлення інформації та часу відгуку ПЗ;

– до засобів інтерактивної взаємодії ПЗ з користувачем (команди, пункти меню, клавіші, курсори);

– до засобів вибору необхідної інформації;

– до перевірки дій та захисту від помилок оператора, а також до довідкової інформації.

В цій частині також наводяться вимоги до аналогових засобів відображення та контролю (прилади вимірювання, індикатори, цифрові табло), що не містять програмного забезпечення.

В другій частині (розділи 4-10) наводяться вимоги до реалізації інтерфейсів користувача для систем з різною функціональністю: системи захисту, системи відображення критичних параметрів, системи відображення колективного користування, комплекси автоматизації, системи передачі інформації.

Третя частина (розділи 11, 12) містить вимоги до розміщення та обладнання робочих місць операторів.

Четверта частина (розділи 13, 14) містить вимоги до безпеки, надійності та здатності до ремонту обладнання робочих місць операторів.

В результаті досліджень вимог стандартів IEC 61772 та IEC 62646, а також нормативного документу NUREG-0700 **можна зробити висновок,** що

вони визначають загальні підходи до проектування інтерфейсів користувача програмного забезпечення КСУ як частини системи взаємодії «людина-машина». Ці вимоги відносяться до всіх етапів життєвого циклу ПЗ КСУ: проектування, реалізації, верифікації, валідації, експлуатації, навчання персоналу. Дотримання вимог цих документів дозволяє створити програмне забезпечення, яке буде відповідати критеріям надійності, захищеності, зручності та ергономічності.

Стандарти кодування MISRA C/C++

Мови програмування С та С++ широко використовуються при створенні програмного забезпечення КСУ. Стандарт IEC 61508 містить рекомендації щодо відповідності коду програм до правил безпечного та ефективного програмування. Прикладом такого стандарту для цих мов є стандарти MISRA C та MISRA C++.

Стандарти кодування MISRA C/C++ розроблені Motor Industry Software Reliability Association – організацією, що створює стандарти розробки програмного забезпечення для автомобільної промисловості [24]. Ці стандарти спрямовані на підвищення функціональної безпеки, інформаційної безпеки та надійності вбудованого ПЗ. Вони використовуються в різноманітних сферах розробки КСУ – космічна діяльність, оборонні технології, автоматизація виробництва та медицина.

Стандарти MISRA C/C++ містить набір правил. Кожне правило має певну категорію: обов'язкове (mandatory), необхідне (requirement) та рекомендоване (advisory). Також вони розподіляються за функціональним призначенням (врахування особливостей компіляторів, уникнення використання деяких функцій, рекомендації щодо найменувань змінних та коментування тощо). Для відповідності ПЗ стандарту обов'язкові та необхідні правила мають бути впровадженні, а рекомендовані правила можуть не виконуватися з обґрунтуванням таких рішень в документації.

Існують програмні інструменти, що використовуються для статичного аналізу коду програми стандарту MISRA: Helix QAC, PVS-Studio, Polyspace [25].

З дослідження змісту стандартів MISRA **можна отримати висновок,** що їх рекомендації підвищують якість та надійність коду ПЗ КСУ АЕС. Високі значення показника якості та надійності необхідні для забезпечення високого рівня функціональної безпеки КСУ АЕС.

Висновки

З метою створення високонадійного та якісного програмного забезпечення комп'ютерних систем керування АЕС, важливих для безпеки, в світі існують стандарти проектування та галузеві нормативні документи. Результатом дослідження стандартів та галузевих нормативних документів, які мають відношення до розробки ПЗ КСУ АЕС, важливих для безпеки є наступне:

– міжнародні стандарти та нормативні документи мають різні рівні спеціалізації. В документах вищого рівня наводяться загальні вимоги до всіх етапів життєвого циклу КСУ та містяться посилання на документи наступного рівня. Документи наступного рівня є більш спеціалізованими і мають відношення до більш вузьких сфер діяльності;

– кожна країна світу може визначати свій набір стандартів та нормативних документів, який вимагається використовувати під час проектування та реалізації КСУ для АЕС;

– в нормативних документах містяться вимоги та рекомендації як щодо організації процесу розробки, так і загальні рекомендації та приклади написання коду програм різними мовами програмування;

– через те, що вимоги розглянутих стандартів мають бути актуальними протягом тривалого часу, ці стандарти не містять формалізованих методик написання коду програм;

– не існує формалізованих методик сертифікації коду на відповідність вимог розглянутих стандартів;

– кожна організація, яка займається проектуванням, розробкою та верифікацією програмного забезпечення КСУ для АЕС, повинна розробити власні методики з застосування вимог та оцінки критеріїв виконання вимог стандартів та нормативів.

Таким чином, виходячи з вишеперерахованого, перспективами подальших досліджень є детальний аналіз вимог міжнародних стандартів та галузевих нормативних документів до програмного забезпечення КСУ АЕС та розробка методики його написання та оцінки відповідності вимогам стандартів.

СПИСОК ЛІТЕРАТУРИ

1. Nuclear power by country. [Електронний ресурс] – Режим доступу: https://en.wikipedia.org/wiki/Nuclear_power_by_country.
2. IEC 61508-2010: Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements. Geneva, International Electrotechnical Commission (IEC), 2010.
3. IEC 61513-2011: Nuclear power plants – Instrumentation and control important to safety – General requirements for systems requirements. Geneva, International Electrotechnical Commission (IEC), 2011.
4. IEC 61226-2009: Nuclear power plants – Instrumentation and control important to safety – Classification of instrumentation and control functions. Geneva, International Electrotechnical Commission (IEC), 2009.
5. IEC 60880-2006: Nuclear power plants – Instrumentation and control systems important to safety – Software aspects for computer-based systems performing category A functions. Geneva, International Electrotechnical Commission (IEC), 2006.
6. IEC 62138-2004: Nuclear power plants –Instrumentation and control important for safety –Software aspects for computer-based systems performing category B or C functions. Geneva, International Electrotechnical Commission (IEC), 2004.
7. IEC 61772:2009: Nuclear power plants – Control rooms – Application of visual display units (VDUs). Geneva, International Electrotechnical Commission (IEC), 2009.
8. IEC 62646-2019: Nuclear power plants – Control rooms – Computer based procedures. Geneva, International Electrotechnical Commission (IEC), 2012.

9. ISO/IEC 27000-2018: Information technology – Security techniques – Information security management systems – Overview and vocabulary. 2018.
10. Keith Stouffer, Victoria Pillitteri, Suzanne Lightman,Marshall Abrams, Adam Hahn. NIST SP 800-82 Revision 2: Guide to Industrial Control Systems (ICS) Security. National Institute of Standards and Technology, 2015.
11. Design of Instrumentation and Control Systems for Nuclear Power Plants: Specific Safety Guide No. SSG-39. Vienna, IAEA, 2016.
12. Safety Classification of Structures, Systems and Components in Nuclear Power Plants: Specific Safety Guide No. SSG-30. Vienna, IAEA, 2014.
13. Application of the Safety Classification of Structures, Systems, and components in Nuclear Power Plants: IAEA-TECDOC-1787. Vienna, IAEA, 2016.
14. ASME NQA-1–2008. Quality Assurance Requirements for Nuclear Facility Applications. An American National Standard. American Society of Mechanical Engineers, 2008.
15. NUREG/CR-6463. Review Guidelines on Software Languages for Use in Nuclear Power Plant Safety Systems. U.S. Nuclear Regulatory Commission, 1996.
16. NUREG-0700 Revision 3. Human-System Interface Design Review Guidelines. U.S. Nuclear Regulatory Commission, 2020.
17. НП 306.2.141–2008. Загальні положення безпеки атомних станцій. Київ, Держатомрегулювання України, 2007.
18. НП 306.2.202-2015. Вимоги з ядерної та радіаційної безпеки до інформаційних та керуючих систем, важливих для безпеки атомних станцій. Київ, Держатомрегулювання України, 2015.
19. СОУ НАЕК 100:2022. Інформаційні та керуючі системи, важливі для безпеки атомних електричних станцій: загальні технічні вимоги. Стандарт державного підприємства «Національна атомна енергогенеруюча компанія «Енергоатом». Київ, ДП НАЕК «Енергоатом», 2022.
20. В. В. Скляр. Обеспечение безопасности АСУТП в соответствии с современными стандартами. Москва – Вологда, Инфра-инженерия, 2018.
21. Daivd J. Smith, Kenneth G. L. Simpson. The Safety Critical Systems Handbook. A Straightforward Guide to Functional Safety IEC 61508 (2010 Edition), IEC 61511 (2015 Edition) and Related Guidance: Forth Edition. Elsevier Ltd, 2016.
22. Chris Hobbs. Embedded Software Development for Safety-Critical Systems: Second Edition. CRC Press, 2020.
23. А. Л. Клевцов, М. А. Ястребенецкий, С. А. Трубчанинов. Компьютерная безопасность информационных и управляющих систем АЭС: нормативная база. Ядерна та радіаційна безпека 4(68), 2015.
24. MISRA website, the official resource for information on MISRA's publications and activities. [Електронний ресурс] – Режим доступу: https://www.misra.org.uk/
25. MISRA C. [Електронний ресурс] – Режим доступу: https://en.wikipedia.org/wiki/MISRA_C

Received (Надійшла) 28.01.2023
Accepted for publication (Прийнята до друку) 12.04.2023

Research of regulatory documents and industry standards for the development of safety-important computer systems for NPP control systems

Boris Vintenko, Oleksii Smirnov, Oleksandr Kovalenko, Serhii Smirnov, Anna Kovalenko

Abstract. Today, one of the main sources of electrical energy are nuclear power plants (NPP). In today's world, digital control systems with widespread use of computers and controllers are used to manage technological processes and ensure safety at nuclear power plants. The safe operation of the NPP depends on the quality and reliability of the software of such systems. In this work, a study of normative documents and standards related to the development of software for computer control systems of nuclear power plants, important for safety, was conducted. **The purpose of the work** is to define standards that can be used by software developers for computerized NPP control systems important for safety. **The object of research** is the process of developing software for computer control systems of nuclear power plants. **The subject is the study** of regulatory documents and industry standards for the development of software for computer control systems of nuclear power plants. **As a result of the study**, the safety criteria of computer control systems were determined, the IEC 61508 and IEC 61513 standards were studied, the IAEA SSG-39 safety instruction was studied, the categories of control functions and safety classes of NPP systems were determined, the standards containing software requirements were studied , user interfaces and MISRA C/C++ coding. **Conclusions**. In order to create highly reliable and high-quality software for computer control systems of nuclear power plants, which are important for safety, there are design standards and industry regulatory documents in the world. The result of the study of standards and industry regulatory documents relevant to the development of software for NPP computer control systems important for safety is the following: international standards and regulatory documents have different levels of specialization. The higher-level documents specify the general requirements for all stages of the life cycle of computer control systems and contain references to the documents of the next level. Documents of the next level are more specialized and relate to narrower fields of activity; each country of the world can determine its own set of standards and regulatory documents, which is required to be used during the design and implementation of computer control systems for nuclear power plants; regulatory documents contain requirements and recommendations both regarding the organization of the development process, as well as general recommendations and examples of writing program code in various programming languages; due to the fact that the requirements of the considered standards must be relevant for a long time, these standards do not contain formalized methods of writing program code; there are no formalized methods of code certification for compliance with the requirements of the considered standards; each organization that is engaged in the design, development and verification of software for computer control systems for nuclear power plants must develop its own methods for applying requirements and evaluating criteria for meeting the requirements of standards and regulations. Thus, it was concluded that the prospects for further research are a detailed analysis of the requirements of international standards and industry normative documents for the software of computer systems of NPP management and the development of a methodology for its writing and assessment of compliance with the requirements of the standards.

Keywords: software, computer control systems, nuclear power plant.