МАГІСТЕРСЬКА РОБОТА

МР. ІПм - 34.00.00.000 ПЗ

Група ІПм-24-2

Люклян Олександр

2025

Івано-Франківський національний технічний університет нафти і газу

Факультет інформаційних технологій

Кафедра інженерії програмного забезпечення

Люклян Олександр Петрович

(прізвище, ім'я, по батькові)

УДК 004.9

(індекс)

МАГІСТЕРСЬКА РОБОТА

IT моделі проєктування промислових систем керування та моніторингу технологічних процесів

(назва роботи)

Інженерія програмного забезпечення

(назва освітньої програми)

121 - Інженерія програмного забезпечення

(шифр і назва спеціальності)

Люклян О.П.

(підпис, ініціали та прізвище здобувача освітнього ступеня)

Науковий керівник Шекета Василь Іванович, д.т.н., професор

(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Допущено до захисту

Завідувач кафедри

доц. Бандура В.В.

(посада) (підпис) (дата) (ініціали та прізвище)

Нормоконтроль

доц. Вовк Р.Б.

(посада) (підпис) (дата) (ініціали та прізвище)

Робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

Івано-Франківськ – 2025

Івано-Франківський національний технічний університет нафти і газу

Факультет інформаційних технологій

Кафедра інженерії програмного забезпечення

Освітній рівень магістр

Спеціальність 121 – Інженерія програмного забезпечення

ЗАТВЕРДЖУЮ:
Зав. кафедрою **ІПЗ**
доц. В.В. Бандура
“ 04 ” вересня 2025 р.

ЗАВДАННЯ

НА МАГІСТЕРСЬКУ РОБОТУ СТУДЕНТУ

Люкляну Олександру Петровичу

(прізвище, ім’я, по-батькові)

1. Тема магістерської роботи “ IT моделі проєктування промислових систем керування та моніторингу технологічних процесів ”

керівник проекту (роботи) Шекета В.І., д.т.н., професор

затверджені наказом закладу вищої освіти від “ 05 ” листопада 2025 р. № 695/7

2. Строк подання студентом проекту (роботи) 15 грудня 2025 р.

3. Вихідні дані до проекту (роботи) Концепції та формальні моделі і методи побудови інформаційних та програмних технологій певного класу

4. Зміст розрахунково - пояснювальної записки(перелік питань, які потрібно розробити)

1. Аналіз предметної області проєктування промислових систем керування та моніторингу ТП
2. Дослідження IT моделей та методології проєктування промислових систем керування
3. Огляд підходів до інтеграції безпеки та захищеності в промислових системах керування
4. Імплементація IT моделей та методології оцінки ризиків кібербезпеки промислових систем

5. Перелік графічного матеріалу (з точним зазначенням обов’язкових креслень)

1. Архітектура типової промислової системи керування (рис. 1.1)
2. Пропонована структура кіберінформованого проектування (рис. 1.2)
3. Спрощене представлення етапів, які виконуються під час аналізу STPA-SafeSec (рис. 1.3)
4. Приклад мережі Байєса (рис. 1.4)
5. Модель технологічного процесу (рис. 2.8)

6. Консультанти розділів проекту (роботи)

Розділ	Консультант	Підпис, дата
Перевірка на плагіат	доц., к.т.н. Вовк Р.Б.	

7. Дата видачі завдання 04 вересня 2025 р.

Керівник _____
(підпис)

Завдання прийняв до виконання_____
(підпис)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Назви етапів магістерської роботи	Строк виконання етапів роботи	Примітка
1	Підбір і вивчення літератури по темі магістерської роботи	17.09.2025	виконано
2	Аналіз предметної області проєктування промислових систем керування та моніторингу ТП	30.09.2025	виконано
3	Дослідження ІТ моделей та методології проєктування промислових систем керування	16.10.2025	виконано
4	Огляд підходів до інтеграції безпеки та захищеності в промислових системах керування	10.11.2025	виконано
5	Імплементація ІТ моделей та методології оцінки ризиків кібербезпеки промислових систем	22.11.2025	виконано
6	Реалізація інтегрованої методології для пріоритизації подій при керуванні та моніторингу технологічних процесів	03.12.2025	виконано
7	Затвердження пояснювальної записки роботи завідувачем кафедри	17.12.2025	виконано

Студент – магістр _____
(підпис)

Керівник роботи _____
(підпис)

АНОТАЦІЯ

Магістерська робота: 77 с., 17 рис., 5 табл., 37 джерела.

Тема: ІТ моделі проєктування промислових систем керування та моніторингу технологічних процесів

Мета магістерської роботи: розроблення та впровадження ІТ-моделей проєктування промислових систем керування і моніторингу технологічних процесів, спрямованих на забезпечення їх функціональної безпеки, надійності та кіберзахищеності.

Об'єкт дослідження: процеси проєктування, керування та моніторингу промислових систем у контексті забезпечення їхньої функціональної безпеки та кіберзахищеності.

Предмет дослідження: інформаційно-технологічні моделі, методи та методології проєктування промислових систем керування і моніторингу, які інтегрують підходи оцінки ризиків, спільного проєктування безпеки та захищеності.

Результати дослідження

В роботі розроблено комплексну методологію забезпечення стійкості промислових систем, що охоплює процеси оцінки ризиків, управління загрозами, визначення критичних точок взаємодії між підсистемами безпеки та захисту,

Висновок

Запропоновано модель оцінки ризиків кібербезпеки на основі Байєсових мереж переконань, що забезпечує адаптивне прогнозування та пріоритизацію подій у промислових технологічних процесах.

ПРОМИСЛОВА СИСТЕМА КЕРУВАННЯ, МОНІТОРИНГ ТЕХНОЛОГІЧНИХ ПРОЦЕСІВ, ІТ МОДЕЛЬ, КІБЕРБЕЗПЕКА, ОЦІНКА РИЗИКІВ, БАЙЄСОВА МЕРЕЖА, СИСТЕМНИЙ АНАЛІЗ, СТІЙКІСТЬ СИСТЕМ, АВТОМАТИЗАЦІЯ ВИРОБНИЦТВА.

ABSTRACT

Master Thesis: 77 pp., 17 fig., 5 tab., 37 sources.

Topic: IT models for designing industrial control systems and monitoring technological processes

The purpose of the master's thesis: development and implementation of IT models for designing industrial control systems and monitoring technological processes aimed at ensuring their functional safety, reliability and cyber security.

Object of research: processes of designing, controlling and monitoring industrial systems in the context of ensuring their functional safety and cyber security.

Subject of research: information technology models, methods and methodologies for designing industrial control and monitoring systems that integrate approaches to risk assessment, joint design of safety and security.

Research results

The paper developed a comprehensive methodology for ensuring the resilience of industrial systems, covering the processes of risk assessment, threat management, identification of critical points of interaction between security and protection subsystems,

Conclusion

A cybersecurity risk assessment model based on Bayesian belief networks is proposed, which provides adaptive forecasting and prioritization of events in industrial technological processes.

INDUSTRIAL CONTROL SYSTEM, MONITORING OF TECHNOLOGICAL PROCESSES, IT MODEL, CYBERSECURITY, RISK ASSESSMENT, BAYESIAN NETWORK, SYSTEMS ANALYSIS, SYSTEMS RESILIENCE, PRODUCTION AUTOMATION.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

CPS - Cyber-Physical Systems

CPT Conditional Probability Table

DAG - Directed Acyclic Graph

ETA - Event Tree Analysis

FMEA - Failure Modes and Effects Analysis

FMVEA - Failure Modes, Vulnerabilities, and Effects Analysis

HCE - High Consequence Events

HMI - Human Machine Interface

JPD - Joint Probability Distribution

MITM - Man in the Middle Attack

SA - Sensitivity Analysis

SIMC - Simple Internal Model Control

ВСТУП

Актуальність теми.

Сучасний етап розвитку промисловості характеризується масштабною цифровою трансформацією, інтеграцією інформаційно-комунікаційних технологій у всі рівні виробничих процесів і переходом до концепції «Індустрія 4.0». Центральне місце в цій трансформації займають промислові системи керування та моніторингу технологічних процесів (ПСК), які забезпечують автоматизацію, аналітику, контроль та оптимізацію виробництва. Проте поряд із підвищенням рівня автоматизації та ефективності функціонування таких систем суттєво зростає складність їхньої архітектури та, як наслідок, ризики порушення безпеки і стійкості.

В умовах розвитку промислового інтернету речей (IIoT), хмарних сервісів, віртуалізації і штучного інтелекту, промислові системи стають відкритими до зовнішніх інформаційних впливів, що зумовлює необхідність перегляду традиційних підходів до їх проєктування. Забезпечення функціональної безпеки, надійності та кіберзахищеності має бути невід'ємною частиною життєвого циклу таких систем — від етапу проєктування до експлуатації.

У роботі розглядається інформаційно-технологічна (IT) модель проєктування промислових систем керування, побудована на принципах кіберінформованого інжинірингу, інтеграції процесів оцінки ризиків і спільного проєктування безпеки та захищеності. Запропоновані підходи спрямовані на підвищення адаптивності промислових систем до загроз і на формування комплексної методології їхнього стійкого функціонування.

Підвищення рівня автоматизації виробничих процесів, зростання кількості взаємопов'язаних кіберфізичних систем і розширення використання відкритих мережевих технологій призвело до виникнення нових викликів у сфері промислової безпеки. Традиційні підходи до проєктування ПСК орієнтовані переважно на функціональну надійність, проте не враховують

сучасних кіберзагроз, які можуть призвести до фізичних ушкоджень обладнання, втрати керованості технологічними процесами або компрометації критичних даних.

Актуальність теми зумовлена потребою у створенні інтегрованих IT-моделей, що поєднують аналіз ризиків, кіберзахист, системну інженерію та методи штучного інтелекту для забезпечення безперервного моніторингу та адаптивного управління технологічними процесами.

У сучасних умовах питання побудови стійких промислових систем, здатних самостійно ідентифікувати, прогнозувати та реагувати на кіберзагрози, є одним із пріоритетів наукових досліджень у сфері автоматизації, комп'ютерних наук та інженерії безпеки. Тому розробка IT-моделей проєктування, що враховують взаємозв'язок між безпекою, надійністю та ефективністю систем керування, має значну практичну та наукову цінність.

Метою магістерської роботи є розроблення та впровадження IT-моделей проєктування промислових систем керування і моніторингу технологічних процесів, спрямованих на забезпечення їх функціональної безпеки, надійності та кіберзахищеності.

Об'єкт дослідження - процеси проєктування, керування та моніторингу промислових систем у контексті забезпечення їхньої функціональної безпеки та кіберзахищеності.

Предмет дослідження - інформаційно-технологічні моделі, методи та методології проєктування промислових систем керування і моніторингу, які інтегрують підходи оцінки ризиків, спільного проєктування безпеки та захищеності.

Завдання дослідження

Для досягнення поставленої мети в роботі вирішено такі основні завдання:

- Провести системний аналіз архітектури, функціональних можливостей та викликів кібербезпеки промислових систем керування.

- Дослідити концептуальні засади кіберінформованого проєктування та визначити основні принципи спільного розроблення безпеки і захищеності.

- Розробити методологію оцінки ризиків кібербезпеки промислових систем на основі системного аналізу та моделей імовірнісних залежностей.

- Створити ІТ-модель вирішення конфліктів між вимогами безпеки і захищеності у процесі проєктування ПСК.

- Розробити інтегровану методологію пріоритизації подій керування та моніторингу технологічних процесів на основі Байєсових мереж переконань.

Методи дослідження

У роботі використано комплекс сучасних наукових методів, серед яких:

- системний аналіз — для вивчення архітектури та структури промислових систем керування;

- методи кіберінформованого інжинірингу — для інтеграції аспектів кіберзахисту у процеси проєктування;

- методи оцінки ризиків (у тому числі кількісні та якісні) — для визначення рівня вразливості системи;

- методи моделювання на основі Байєсових мереж переконань — для опису ймовірнісних залежностей між подіями;

- методи експертного аналізу та моделювання сценаріїв — для формування рішень щодо усунення конфліктів між вимогами безпеки і захищеності;

- емпіричне моделювання та комп’ютерна верифікація — для перевірки працездатності запропонованих моделей.

Наукова новизна отриманих результатів

Розроблено інтегровану ІТ-модель проєктування промислових систем керування, що поєднує підходи кіберінформованого інжинірингу, оцінки ризиків і спільного проєктування безпеки та захищеності. Удосконалено метод аналізу та вирішення конфліктів між вимогами безпеки й захищеності, який базується на принципах системного процес-аналізу та навчання на основі конфліктів.

Практичне застосування результатів

Отримані результати мають прикладне значення для підприємств промислової автоматизації, IT-компаній і науково-дослідних центрів. Запропоновані моделі та методології можуть бути використані:

- при розробленні архітектурних рішень для SCADA- та DCS-систем із вбудованими засобами кіберзахисту;

- у процесі аудиту безпеки промислових систем і формування політик управління ризиками;

- для підтримки прийняття рішень у реальному часі під час моніторингу технологічних процесів.

Структура магістерської роботи. Представлена робота складається зі вступу, трьох розділів та висновків. Загальний обсяг роботи становить 77 сторінок, і містить 17 рисунків, 5 таблиць, перелік використаних джерел із 34 позицій.

РОЗДІЛ 1. АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ ПРОЄКТУВАННЯ ПРОМИСЛОВИХ СИСТЕМ КЕРУВАННЯ ТА МОНІТОРИНГУ ТЕХНОЛОГІЧНИХ ПРОЦЕСІВ

1.1. Архітектура, функціональність та виклики кібербезпеки промислових систем керування

Промислові системи керування (ПСК) являють собою вбудовані системи, що здійснюють моніторинг та оперативне управління виробничими (технологічними) процесами. Вони критично важливі для забезпечення надійної, безпечної та захищеної експлуатації промислових об'єктів та критичної інфраструктури, зокрема в секторах енергетики, електроенергетики, хімічної та ядерної промисловості, а також систем водопостачання та водовідведення. Ці системи, що мають критичне значення для безпеки (safety-critical), інтегрують різноманітні технологічні рішення та процеси, спрямовані на контроль та регулювання складних промислових операцій. Архітектура ПСК передбачає інтеграцію апаратних і програмних компонентів, зокрема:

- Датчики та виконавчі механізми
- Програмовані логічні контролери (ПЛК)
- Системи диспетчерського керування та збору даних (SCADA)

Дана інтеграція забезпечує автоматизацію та оперативне управління промисловими діями, що сприяє підвищенню їхньої надійності, безпеки (safety) та захищеності (security). Компоненти взаємодіють для моніторингу технологічних змінних (таких як швидкість потоку, рівень рідини, тиск, температура) та прийняття рішень у реальному часі для регулювання операцій.

Типова архітектура ПСК поділяється на кілька функціональних рівнів, де кожен рівень виконує певні завдання, а інформаційний потік рухається знизу (від процесу) вгору (до корпоративного управління) і навпаки.

Рис. 1.1. Архітектура типової промислової системи керування

1. Рівень об'єкта керування (Field Level)

Це найнижчий, фізичний рівень, який безпосередньо взаємодіє з промисловим процесом. Компоненти: Датчики (Sensors), Виконавчі механізми (Actuators), приводи, клапани, насоси.

Функція: Збір вимірюваних змінних процесу (температура, тиск, потік) та виконання фізичних команд, надісланих від контролерів.

Приклад: Термопара вимірює температуру, а регулюючий клапан відкривається/закривається за командою.

2. Рівень керування (Control Level)

На цьому рівні відбувається безпосереднє автоматичне керування технологічним процесом у реальному часі. Компоненти: програмовані логічні контролери (ПЛК) (PLC), розподілені системи керування (DCS), контролери автоматизації процесів (PAC).

Функція: Виконання логіки керування, обробка даних із датчиків, підтримка параметрів процесу в заданих межах, керування виконавчими механізмами.

Приклад: ПЛК безпосередньо приймає рішення про ввімкнення насоса чи зміну заданого значення.

3. Рівень диспетчерського керування (Supervisory Control Level)

Цей рівень забезпечує моніторинг, візуалізацію та взаємодію оператора з процесами. Компоненти: Системи SCADA (Supervisory Control and Data Acquisition), Інтерфейс Людина-Машина (HMI), сервери даних.

Функція: Збір даних із багатьох ПЛК, архівація даних, відображення стану процесу для оператора, можливість ручного втручання та встановлення нових заданих значень (уставок).

Приклад: Оператор контролює процес на HMI-панелі або робочій станції SCADA і може змінити виробничий рецепт.

4. Рівень виробничого управління (Manufacturing Operations Management - MOM) інтегрує керування процесами з бізнес-плануванням. Компоненти: Системи управління виробничими процесами (MES), системи управління лабораторною інформацією (LIMS).

Функція: Оптимізація виробництва, планування графіків, управління ресурсами, контроль якості, відстеження партій продукції та управління запасами.

Приклад: MES-система отримує замовлення з рівня ERP та генерує відповідні виробничі завдання для SCADA/ПЛК.

5. Корпоративний Рівень (Enterprise Level)

Найвищий рівень, орієнтований на бізнес-стратегію та планування. Компоненти: системи планування ресурсів підприємства (ERP), корпоративні бази даних, бізнес-аналітика.

Функція: Довгострокове планування, фінанси, управління ланцюгом поставок, прийняття стратегічних рішень.

Приклад: ERP-система використовує дані про виробництво, отримані з рівня MOM, для фінансового обліку та прогнозування попиту.

1.1.1. Програмовані логічні контролери і SCADA системи

ПЛК – це міцні, твердотільні обчислювальні пристрої, спеціально розроблені для виконання завдань керування з жорсткими вимогами до часу реакції (real-time control). Вони обробляють вхідні сигнали від датчиків та інших пристроїв і генерують вихідні сигнали для керування промисловим обладнанням та процесами на основі заздалегідь визначених логічних алгоритмів.

Завдяки своїй гнучкості та можливості перепрограмування, ПЛК широко застосовуються в промисловості. Інженери мають можливість коригувати їхнє програмне забезпечення для адаптації до змін системних вимог без необхідності значної модифікації чи заміни апаратного забезпечення. Така адаптивність оптимізує реконфігурацію системи, мінімізуючи час простою та експлуатаційні витрати.

Інтеграція ПЛК з інтерфейсами людина-машина (HMI) та системами SCADA підвищує рівень безпеки промислових середовищ, включаючи механізми безпечних блокувань та процедури аварійного вимкнення для захисту обладнання та персоналу. У разі виявлення відмови, ПЛК можуть оперативно виконувати заздалегідь визначені протоколи безпеки, знижуючи потенційні ризики.

Системи SCADA забезпечують можливості моніторингу, керування та збору даних у реальному часі. Вони агрегують дані від датчиків, обробляють їх та представляють операторам у формі зрозумілих звітів та візуалізацій. Це дозволяє операторам приймати обґрунтовані рішення, оптимізувати процеси, забезпечувати безпеку та підвищувати ефективність. SCADA-системи є критичними для швидкої ідентифікації проблем та негайного втручання.

Сучасні SCADA-системи еволюціонували завдяки інтеграції Інтернету речей (IoT) та штучного інтелекту (AI), що дає змогу проводити аналіз

великих обсягів даних у режимі реального часу, необхідний для предиктивного обслуговування, прогнозування відмов системи та оптимізації процесів. Ці технологічні досягнення сприяють скороченню системних простоїв та підвищенню стійкості.

1.1.2. Виклики кібербезпеки та шляхи їх вирішення

Незважаючи на переваги, ПСК стикаються зі значними викликами, головним з яких є кібербезпека. Кіберзагрози становлять істотний ризик, оскільки вони можуть порушити операції, загрожувати безпеці та призводити до значних фінансових втрат або навіть людських жертв.

Складність, взаємозв'язок операційних технологій (ОТ) та інформаційних технологій (ІТ), а також можливості дистанційного керування, роблять ці системи вразливими до успішних кібератак.

Наведемо приклади інцидентів. Відомі атаки, такі як Stuxnet (перепрограмування ПЛК), інциденти з очисними спорудами у Квінсленді (маніпуляція SCADA) та атаки BlackEnergy на українську електромережу (компрометація SCADA), демонструють потенційні катастрофічні фізичні наслідки, які відрізняють кібератаки на ПСК від їхніх ІТ-аналогів.

Захист ПСК вимагає впровадження надійних механізмів безпеки, захищеності та стійкості. Успішні кібератаки на ПСК мають прямі фізичні наслідки, включаючи пошкодження обладнання, забруднення довкілля, травми чи смерть. З огляду на це, урядові структури співпрацюють з промисловістю та науковими колами для розробки стандартів та нормативних рамок, як-от NIST Cybersecurity Framework та ISA/IEC 62443, для вирішення проблем кібербезпеки ПСК.

1.2. Концептуальна основа кіберінформованого проектування

Для системного вирішення цих проблем пропонується та реалізується інноваційний підхід – кіберінформоване проектування (КІП). Цей підхід

інтегрує практики кібербезпеки та інженерії на ранніх етапах проектування та розробки системи.

КІП реалізується через ключові концепції:

- Спільне проектування безпеки (safety) та захищеності (security) - одночасний розгляд обох аспектів.

- Оцінка ризиків кібербезпеки - систематична ідентифікація та аналіз загроз.

- Стійке проектування (resilient design), розробка систем, здатних витримувати атаки та швидко відновлюватися.

Ці концепції є фундаментальними для створення критичних ПСК, які є не лише безпечними та захищеними, але й демонструють високу надійність та стійкість до постійно еволюціонуючих кіберзагроз.

Кіберінформоване проектування (КІП) (Cybersecurity-Informed Design, CID) є вдосконаленим методологічним підходом, спрямованим на інтеграцію принципів кібербезпеки на етапах проектування та розробки систем критичної інфраструктури.

КІП являє собою новітню архітектурну рамку кібербезпеки. Її ключова мета полягає у проактивному захисті критичної інфраструктури (зокрема енергетичної, електроенергетичної, хімічної, водогосподарської та ядерної промисловості) від постійно еволюціонуючих кіберзагроз. КІП – це підхід, який характеризує ризики, що виникають внаслідок впровадження цифрових комп'ютерних систем у традиційно аналогове середовище, і пропонує стратегію застосування інженерних процесів управління ризиками для мінімізації цих ризиків. Він включає методи, що забезпечують врахування кіберризиків протягом усього життєвого циклу проектування, а також техніки, які дозволяють усунути кіберризики за допомогою інженерних методів.

Фреймворк КІП фокусується на ідентифікації актуальних кіберзагроз у критичній інфраструктурі та їх проактивному вирішенні на початкових етапах системного проектування та розробки.

Підхід вимагає тісної співпраці між експертами з кібербезпеки та інженерами-проектувальниками для спільного аналізу, виявлення та пріоритизації потенційних вразливостей і загроз. Раннє виявлення загроз дозволяє впровадити надійні інженерні заходи та стратегії для ефективного зниження кіберризиків. Інтеграція практик кібербезпеки в інженерний процес сприяє створенню систем, які є одночасно безпечними (safety), захищеними (security) та надійними (reliable).

КІП вимагає від інженерів суворого дотримання та інтеграції вимог і рекомендацій з кібербезпеки протягом усього інженерного циклу.

Крім цього, ключовими елементами КІП є:

- Моніторинг у реальному часі: впровадження механізмів постійного моніторингу системи.

- Механізми відновлення: розробка протоколів відновлення (resilience) для швидкого реагування та пом'якшення наслідків кібератак чи відмов.

Проактивне вирішення питань спільного проектування безпеки та захищеності, управління кіберризиками та відповідність галузевим нормам і стандартам дозволяє організаціям ефективніше захищати критичні системи та забезпечувати їх стійкість в умовах динамічного ландшафту кіберзагроз.

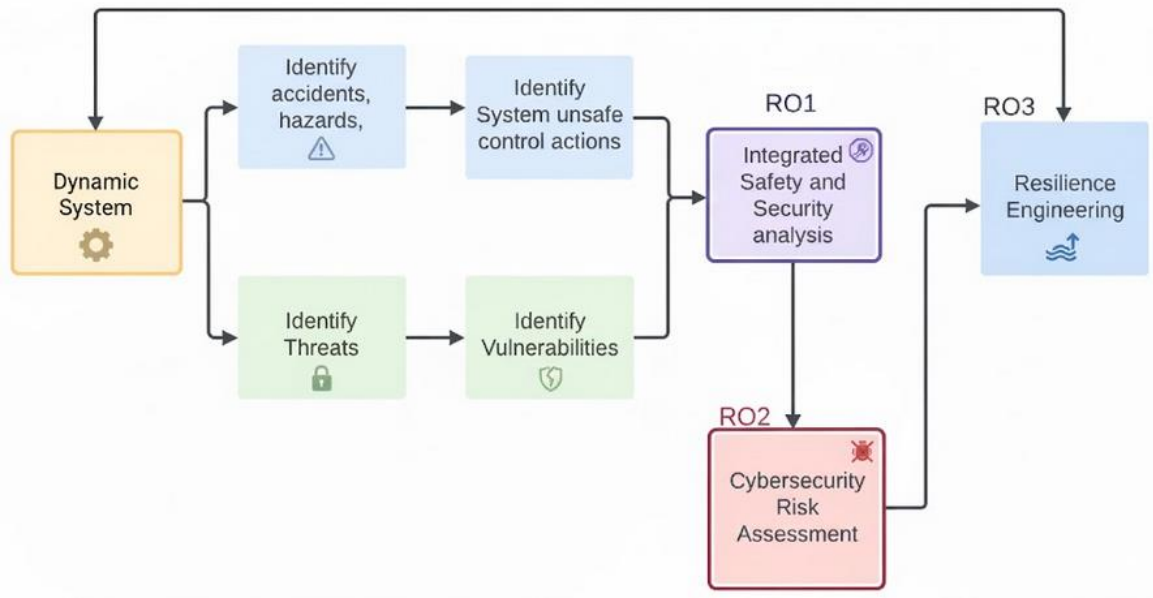


Рис. 1.2. Пропонована структура кіберінформованого проектування

Запропонована структура КІП, що застосовується в даному дослідженні, складається з трьох основних фаз:

- Спільне проектування безпеки та захищеності (Co-design of Safety and Security).

- Оцінка ризиків кібербезпеки (Cybersecurity Risk Assessment).

- Стійке проектування (Resilient Design).

Ці фази (RO1, RO2 та RO3 відповідно, згідно з дослідницькими цілями) формують методологічну основу для створення стійких критичних систем.

1.3. Комплексна методологія забезпечення стійкості промислових систем керування засобами кіберінформованого проектування

1.3.1. Спільне проектування безпеки та захищеності

Безпека (Safety) та захищеність (Security) є критично важливими детермінантами, що забезпечують безперебійне та захищене функціонування промислових систем керування (ПСК). Проектування безпеки зосереджується на аналізі потенційних системних аварій, які можуть призвести до небезпечних станів та збитків. Його основна мета – запобігання небажаним наслідкам, таким як пошкодження обладнання, фінансові втрати чи втрата людського життя. На противагу цьому, проектування захищеності концентрується на ідентифікації та мінімізації ризиків, загроз та вразливостей, притаманних цільовій системі.

Спільне проектування безпеки та захищеності (Co-design of Safety and Security) визначається як інтеграція цих двох аспектів на початкових фазах інженерного проектування та розробки системи. Традиційно, в інженерній практиці, безпека розглядалася як найвищий пріоритет, тоді як захищеність мала вторинний статус. При створенні ПСК ці домени часто розглядалися ізольовано, де інженери та фахівці з безпеки функціонували автономно. На сучасному етапі науковці та промисловість усвідомили необхідність

об'єднання практик проектування безпеки та захищеності в єдиний, цілісний підхід для забезпечення загальної безпеки та захищеності ПСК.

Інтеграція безпеки та захищеності, проте, може призводити до конфліктних обмежень, що є досі не повністю вирішеною проблемою як у промисловості, так і в академічних колах. Згідно з дослідженнями, виявлення та мінімізація таких конфліктів залишається недостатньо вивченою.

Приклад конфлікту. На об'єкті критичної інфраструктури, як-от атомна електростанція, цілі безпеки вимагають забезпечення швидкої евакуації (легкодоступні аварійні виходи, мінімальні бар'єри). Водночас, цілі захищеності вимагають обмеження доступу до чутливих зон (контроль доступу, системи спостереження). У критичній ситуації (наприклад, пожежа), забезпечення легкого доступу до аварійних виходів з міркувань безпеки може одночасно полегшити несанкціоноване проникнення зловмисника, ставлячи під загрозу захищеність ядерного об'єкта. Нерозв'язані конфлікти такого роду підвищують ризик експлуатації критичних систем.

Дане дослідження фокусується на спільному проектуванні на ранніх фазах розробки, акцентуючи увагу на ідентифікації, аналізі та вирішенні конфліктних обмежень. Для цього пропонується інтеграція підходу STPA-SafeSec для комплексного аналізу безпеки та захищеності та техніки навчання на основі конфліктів (CDCL).

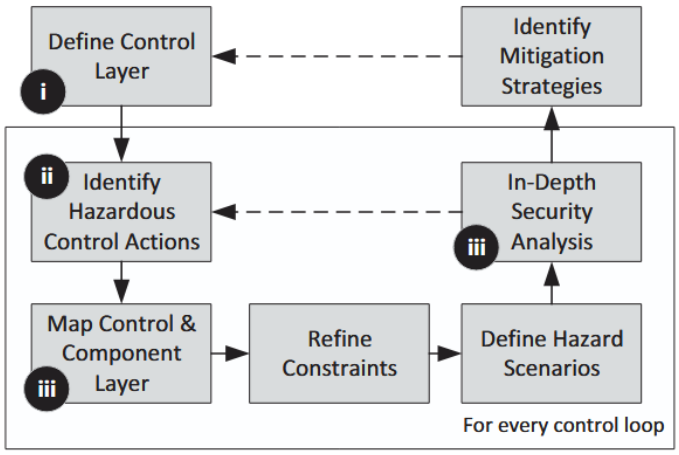


Рис. 1.3. Спрощене представлення етапів, які виконуються під час аналізу STPA-SafeSec

Суцільні стрілки на рис. 1.3 вказують на послідовність, у якій виконуються етапи. Пунктирні стрілки позначають місця, де відбувається ітерація STPA-SafeSec. Чорні кола вказують на етапи, де застосовуються розширення STPA-SafeSec. Спочатку визначається рівень керування для всієї системи, що складається з різних контурів керування. Далі детально аналізується кожен контур керування з метою визначення сценаріїв, за яких системні недоліки або зловмисні дії можуть спричинити системні небезпеки (system hazards). На основі сукупності всіх сценаріїв може бути визначено найбільш ефективні стратегії мінімізації ризиків у системі.

STPA-SafeSec - систематична техніка, що використовує підхід «зверху-вниз» для інтегрованого аналізу безпеки та захищеності, охоплюючи аномальну системну поведінку через відмови взаємодії компонентів.

CDCL (Conflict-Driven Clause Learning) - алгоритм вирішення задач булевої задовольняльності (SAT), що демонструє високу ефективність в аналізі та розв'язанні конфліктів.

Загальна мета полягає у підвищенні надійності, стійкості та живучості ПСК.

1.3.2. Оцінка ризиків кібербезпеки

Забезпечення захищеності критичної інфраструктури є першочерговим завданням в умовах взаємопов'язаного та технологічно розвиненого суспільства. Захист цих критичних активів вимагає ретельної оцінки ризиків кібербезпеки. Однак, через обмеженість ресурсів кібербезпеки та дефіцит кваліфікованих експертів, повне усунення всіх можливих кіберризиків, які зловмисники можуть використати для спричинення серйозних наслідків, є неможливим. Це призводить до ситуації, коли державний та приватний сектори змушені діяти реактивно. Наслідки успішних атак на ці системи є катастрофічними, що вимагає максимально можливого захисту.

Критично важливим є аналіз, виявлення та пріоритизація подій з високими наслідками (High-Consequence Events, HCE) на ранніх етапах

проектування. НСЕ – це події, що мають найбільш серйозний вплив на функціонування системи. НСЕ впливають на критичні функції організації, паралізуючи її повсякденну діяльність.

НСЕ впливають на життєво важливі компоненти та процеси (наприклад, реакторний блок, тиск, температура), що може призвести до пошкодження об'єкта, зупинки виробництва, екологічного забруднення, фінансових збитків, травм або смерті. Існуючі методи оцінки ризиків кібербезпеки не повною мірою вирішують ці проблеми, що зумовлює необхідність вдосконаленого підходу.

Це дослідження пропонує та реалізує підхід до оцінки ризиків кібербезпеки, що інтегрує концепцію наслідково-орієнтованого кіберінформованого проектування (CCE) та мережі Байєса (BBN) з аналізом чутливості (SA).

CCE (Consequence-driven Cyber-informed Engineering) - підхід «зверху-вниз», що фокусується на ідентифікації НСЕ, визначенні шляхів використання системи зловмисником для спричинення НСЕ та розробці стратегій мінімізації. На відміну від існуючого CCE, наш підхід мінімізує залежність від людських/експертних знань при пріоритизації НСЕ, використовуючи BBN та SA.

BBN (Bayesian Belief Networks) - графова модель, що використовується для представлення та аналізу ймовірнісних взаємозв'язків між визначеним набором змінних, моделюючи невизначеність у системі.

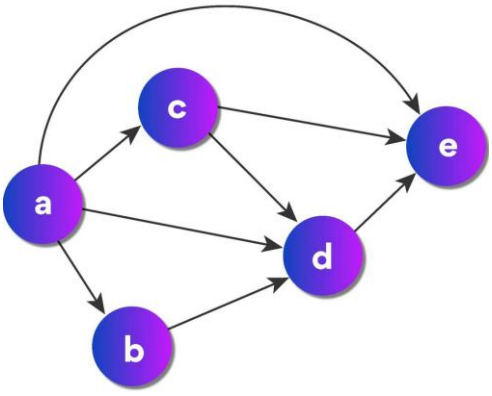


Рис. 1.4. Приклад мережі Байєса

SA (Sensitivity Analysis) використовується для валідації моделі BBN шляхом аналізу та виявлення критичних вузлів у мережі.

Моделі BBN та SA розроблені на основі чотирьох критичних факторів ризику кібербезпеки: безпека (Safety), цілісність (Integrity), доступність (Availability) та вартість (Cost) (SIAC). Логіка вибору критеріїв SIAC полягає в тому, що в контексті критичної інфраструктури основною метою будь-якої ворожої діяльності є порушення саме цих ключових аспектів. Запропонована структура поділена на дві частини:

- Фаза пріоритизації наслідків - виявлення та пріоритизація HCE.

- Фаза наслідково-орієнтованого цільового впливу - аналіз та ідентифікація загроз безпеці та демонстрація шляхів використання системи для ініціювання HCE.

1.3.3. Сутність процесів стійкого проектування

Стійке проектування (Resilient Design) в ПСК полягає у створенні систем, які здатні витримувати та відновлюватися після збоїв або атак, мінімізуючи час простою та ризики для безпеки. Стійка система проактивно підтримує свою функціональність навіть у деградованому стані, забезпечуючи безперервність критичних процесів і функцій. Ключовими викликами стійкого проектування є своєчасне виявлення атак/відмов та швидке відновлення. Наприклад, на атомній електростанції затримка у виявленні атаки може призвести до ядерної аварії.

Недоліки існуючих підходів:

1. Надмірність (Redundancy) - дублювання критичних компонентів. Основний недолік, окрім високої вартості, полягає в тому, що ідентична конфігурація основної та резервної систем робить їх вразливими до однієї й тієї ж атаки.

2. Машинне Навчання (ML) часто призводить до хибнопозитивних/ хибнонегативних результатів і має затримку у виявленні, що є критичним для швидкого відновлення.

3. Фокус на кіберчастині, оскільки більшість досліджень концентруються на моніторингу кіберчастини (IT) кібер-фізичних систем (CPS), ігноруючи фізичний або процесовий домен. Проте вплив домену керування процесами на стійкість є зростаючою сферою, оскільки порушення фізичного процесу призводить до змін у динаміці, які можуть бути виявлені механізмами, орієнтованими на процес.

У відповідь на ці виклики, пропонується та реалізується вдосконалений підхід STL-Autotuning, що поєднує концепцію тимчасової логіки сигналів (STL) та техніку автоналаштування для підвищення стійкості ПСК через моніторинг критичних процесів у реальному часі та автоматичне відновлення.

STL (Signal Temporal Logic) - логічний формалізм для специфікації часових властивостей сигналів із дійсними значеннями. STL забезпечує моніторинг у режимі реального часу та відстеження траєкторій стану системи для виявлення порушень. Використовує кількісну семантику для вимірювання ступеня, в якому траєкторія може бути зміщена в часі без впливу на задоволення або порушення специфікації STL.

Автоналаштування (Autotuning) - добре відомий механізм для створення надійних систем, де ПІД-контролер проактивно здійснює самосвідомість та самооптимізацію, сприяючи автоматичному відновленню процесів до нормального робочого стану.

Ми використовуємо правило SIMC- PID для механізму автоналаштування. SIMC-PID відомий своєю стійкістю в роботі як зі стійкими, так і з нестійкими процесами. Механізм реалізується з моделлю другого порядку плюс затримка часу (SOPTD) для автоматичного відновлення системи при порушенні умов безпеки.

Механізм автоналаштування активується, коли результат кількісної семантики STL для критичного процесу перевищує заздалегідь встановлений поріг θ. Цей поріг визначає ступінь порушення специфікації, що здатний

вплинути на цілісність, доступність та безпеку системи, і встановлюється експертом на основі експериментальних даних.

Запропонований підхід є спробою інтеграції моніторингу на основі STL з механізмом автоналаштування. Ця інтеграція дозволяє захоплювати сліди поведінки системи в режимі реального часу, забезпечуючи відновлення системи у разі відхилень від стандартних робочих шаблонів, що потенційно погіршують функціональність. Така інноваційна комбінація моніторингу та автоналаштування критичних процесів є фундаментальною для створення надійних, стійких та живучих систем.

Висновки до розділу

В даному розділі проведено здійснено системний аналіз предметної області проєктування промислових систем керування та моніторингу технологічних процесів, розглянуто їх архітектуру, функціональні компоненти, а також специфічні виклики, пов’язані з кібербезпекою.

Встановлено, що сучасні ПСК, засновані на використанні програмованих логічних контролерів (PLC) та SCADA-систем, є складними кіберфізичними структурами, вразливими до атак на рівні даних, комунікацій і керування. Зростання взаємозв’язку між рівнями IT- та OT-інфраструктури створює нові вектори атак, що потребують інтеграції кіберзахисту вже на етапі проєктування.

Проаналізовано концептуальні основи кіберінформованого проєктування, які поєднують традиційні підходи системної інженерії з моделями кібербезпеки. Визначено принципи спільного проєктування безпеки та захищеності (“co-engineering”), що дозволяють враховувати вимоги функціональної безпеки одночасно із вимогами інформаційної безпеки.

Сформовано комплексну методологію забезпечення стійкості промислових систем, яка включає етапи оцінки ризиків, управління

загрозами та побудову процесів стійкого проєктування. Показано, що поєднання моделей ризиків із процесним аналізом забезпечує адаптивність ПСК до змін зовнішнього середовища та кіберзагроз.

РОЗДІЛ 2. ДОСЛІДЖЕННЯ ІТ МОДЕЛЕЙ ТА МЕТОДОЛОГІЇ ПРОЄКТУВАННЯ ПРОМИСЛОВИХ СИСТЕМ КЕРУВАННЯ ДЛЯ ЗАБЕЗПЕЧЕННЯ ЇХ БЕЗПЕКИ ТА ЗАХИЩЕНОСТІ

2.1. Аналіз та вирішення конфліктів умов безпеки та захищеності для промислових систем керування

Забезпечення безпеки (safety) та захищеності (security) є критично важливими властивостями промислових систем керування (ПСК). Необхідною умовою ефективного функціонування ПСК є інтеграція цих двох аспектів, що запобігає підриву цілей безпеки цілями захищеності, і навпаки. Проте, спільне проектування безпеки та захищеності може спричинити виникнення конфліктних вимог або порушень, які можуть негативно вплинути на нормальну поведінку системи. Ідентифікація, аналіз та вирішення конфліктів, що виникають внаслідок спільного проектування, залишаються значною та недостатньо вивченою проблемою в контексті критичних систем (ПСК). Для вирішення цієї проблеми у даній роботі запропоновано методологію STPA-SafeSec-CDCL. Запропонований підхід поєднує техніку STPA-SafeSec для інтегрованого аналізу безпеки та захищеності, а також метод навчання на основі конфліктів (CDCL) для виявлення, аналізу та розв'язання конфліктів. Конфліктні обмеження кодуються в задачі булевої задовольняльності (SAT). Ефективність фреймворку демонструється шляхом його застосування до моделі процесу — еталонної моделі, розробленої спеціально для дослідження промислових процесів керування. Запропонована методологія може бути застосована на ранніх етапах проектування та розробки системи, виходячи за межі фази аналізу вимог, з метою підвищення системної надійності, стійкості та живучості.

Розвиток технологій та впровадження парадигми Індустрії 4.0 суттєво підвищили складність проектування та розробки кібер-фізичних систем

(CPS). CPS інтегрують апаратні та програмні ресурси для обчислювальних, комунікаційних та керуючих цілей, які спільно проектуються з фізично інженерними компонентами. Типовим прикладом CPS є промислові системи керування (ПСК), які здійснюють моніторинг та управління фізичними процесами за принципом зворотного зв'язку, де фізичні процеси впливають на обчислення і навпаки. Глибока інтеграція дискретних обчислень та безперервних фізичних процесів створює значні інженерні виклики, зокрема у сфері спільного проектування вимог безпеки та захищеності.

Безпека та захищеність є двома фундаментальними властивостями ПСК. На ранніх етапах проектування CPS вони розглядалися як ізольовані сутності. Проектування безпеки вивчає потенційні системні аварії, здатні призвести до небезпечних ситуацій та збитків. У контексті ПСК втрати класифікуються на прийнятні та неприйнятні. Методології безпеки спрямовані на запобігання неприйнятним втратам, таким як пошкодження обладнання, людські жертви або значні фінансові збитки.

Проектування захищеності фокусується на мінімізації ризиків, загроз та вразливостей, притаманних цільовій системі. CPS класифікуються на системи, критичні для безпеки, та системи, критичні для захищеності. У системі, критичній для безпеки, пріоритет віддається безпеці, а в протилежному випадку — захищеності, причому для їх аналізу традиційно використовувалися різні інструменти моделювання.

Інтеграція безпеки та захищеності в ПСК є обов'язковою для комплексного захисту системи від потенційних аварій та атак. Проте, комбінування цих вимог іноді призводить до конфлікту, що залишається недостатньо розв'язаною проблемою як у науковому середовищі, так і в промисловості. У багатьох дослідженнях щодо спільного проектування, відзначають, що сфери виявлення та вирішення конфліктних вимог безпеки та захищеності є не повністю вивченими. Нерозв'язані конфліктні вимоги створюють у ПСК вразливі стани, які можуть бути експлуатовані кіберзлочинцями.

Історично аналіз безпеки критичних CPS виконувався з використанням таких підходів, як моделювання мережею Петрі з часом, при цьому багато досліджень слідували шляхом відокремлення безпеки від захищеності. Концепція інтегрованого аналізу безпеки та захищеності отримала широке визнання з акцентом на уніфікаційні підходи, де безпека та захищеність розглядаються як окремі сутності, що об'єднуються протягом життєвого циклу розробки системи.

Дана робота спрямована на аналіз безпеки та захищеності ПСК, концентруючись на спільному проектуванні, ідентифікації та вирішенні конфліктних обмежень, які можуть призвести до відмови системи або кібератак. Головна мета полягає у підвищенні надійності, стійкості та живучості ПСК.

Для досягнення цієї мети пропонується інтеграція підходу STPA-SafeSec для аналізу безпеки та захищеності з методом навчання на основі конфліктів (CDCL) для виявлення, аналізу та вирішення конфліктів.

STPA-SafeSec - це систематична техніка, що використовує підхід «зверху-вниз» для виконання інтегрованого аналізу безпеки та захищеності, охоплюючи аномальні поведінки системи через відмови взаємодії компонентів.

Дане дослідження фокусується виключно на аналізі та вирішенні конфліктів, що виникають з обмежених умов безпеки та захищеності, і не охоплює всі аспекти конфліктів, пов'язаних з інтеграцією, наприклад, конфлікти, що стосуються конфіденційності та/або доступності. Реалізація здійснюється за допомогою скрипту на мові Python.

2.2. Огляд сучасних підходів до інтеграції безпеки та захищеності в промислових системах керування

Наукові дослідження активно розглядають проблему інтеграції безпеки (safety) та захищеності (security) у промислових системах керування.

2.2.1. Спільне проектування та документація вимог

Ряд наукових праць пропонує методології для забезпечення узгодженості між вимогами безпеки та захищеності.

В роботі [3] дослідили взаємозв'язок між безпекою та захищеністю в ПСК. Їхня робота зосередилася на захисті системного програмного забезпечення та операційного середовища шляхом пропозиції імплементації захисної оболонки при створенні програм забезпечення захищеності.

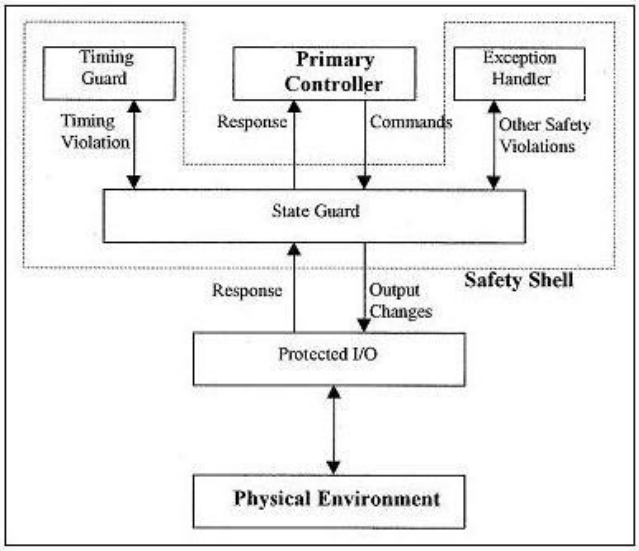


Рис. 2.1. Архітектура захисної оболонки

Незважаючи на існування численних, добре усталених методологій та технік для вирішення проблем безпеки на етапі розробки, вони, як правило, не розглядають безпеку та захищеність як два взаємопов'язані аспекти однієї й тієї ж проблеми. Підхід, під назвою «захисна оболонка» (safety shell) (рис. 2.1), що базується на архітектурній моделі, яка уможливлює проектування систем керування, демонструє разючу схожість із типовою «моделлю цибулини» (onion model) забезпечення захищеності. Ця концепція ґрунтується на реалізації елемента проектування «спочатку тестуй» (test first) для запобігання виникненню небезпечних ситуацій, що має на меті виявлення небезпечної ситуації на її початковій стадії. Шляхом

«попереднього тестування» апаратний процесор або програмна оболонка або підтверджує (validate), або відхиляє (invalidate) поточну та/або бажану дію.

В роботі [4] представили інтегровану модель для вимог безпеки та захищеності кібер-фізичних систем (CPS). Модель ґрунтується на інженерії вимог, управлінні ризиками та документації доказів для підтримки процесу пересертифікації. В дослідженні [5] запропонували процес інтеграції безпеки та захищеності відповідно до стандарту ISO 26262 (який надає настанови щодо розробки безпечних автомобільних застосувань). В [6] розробили підхід, що виходить за межі простої інтеграції, фокусуючись на верифікації вимог безпеки та захищеності з метою виявлення системних залежностей та відмов.

2.2.2. Інтегрований аналіз ризиків

З огляду на зростаючу взаємопов'язаність та складність CPS, наукова спільнота визнала необхідність об'єднання аналізу ризиків, пов'язаних як з безпекою, так і з захищеністю, що раніше виконувалися незалежно.

В дослідженні [5] запропонували метод аналізу ризиків, що одночасно розглядає безпеку та захищеність на основі підходу аналізу системних теоретичних процесів (STPA). Ця техніка була застосована до медичного пристрою (інсулінового насоса) для виявлення аварій, які неможливо запобігти за допомогою функціональної безпеки.

В роботі [6] представили підхід S-cube до спільної оцінки ризиків, який є корисним на різних етапах розробки системи.

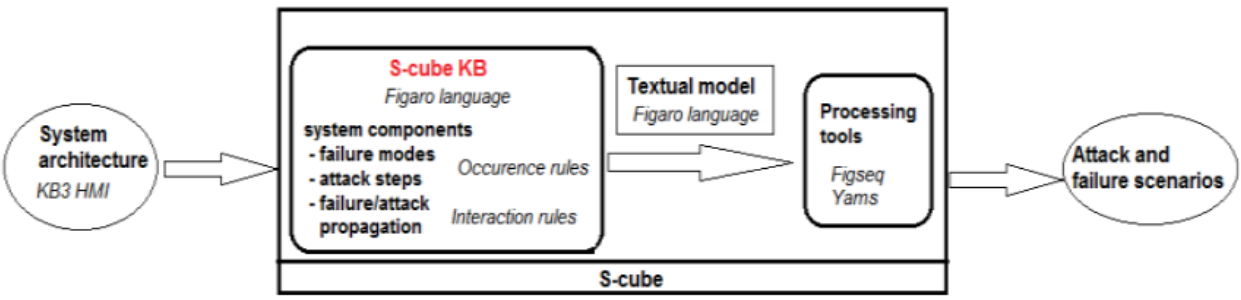


Рис. 2.2. Підхід S-cube

Підхід S-cube, представлений на рис. 2.2, приймає на вхід архітектуру системи та генерує на виході сценарії атак та відмов, які, ймовірно, можуть статися в цій системі і призвести до заданої небажаної події, пов'язаної з проблемами безпеки (safety). Підхід S-cube спирається на базу знань (S-cube KB), яка акумулює експертні знання щодо промислових систем керування і, зокрема, систем SCADA, а також пов'язаних з ними ризиків безпеки та захищеності. S-cube KB є предметно-орієнтованою мовою (Domain Specific Language, DSL), що дозволяє описувати типові компоненти цифрових промислових інфраструктур із врахуванням аспектів безпеки та захищеності (таких як автентифікація, контроль доступу, надмірність). Кожен компонент асоційований із режимами атак та відмов, які можуть на ньому виникнути.

Загальні моделі S-cube KB інстанціюються (конкретизуються) відповідно до вхідної архітектури системи та обробляються обчислювальними механізмами, які автоматично генерують сценарії атак та відмов.

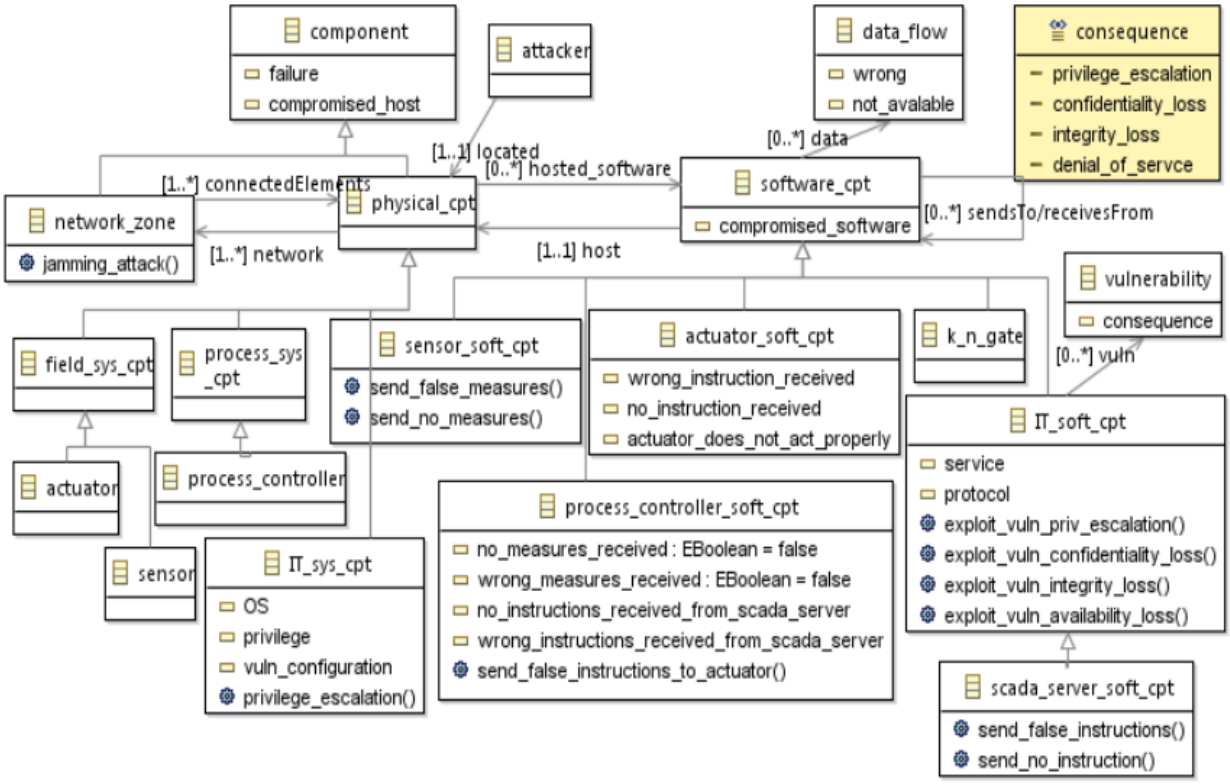


Рис. 2.3. Метамодель S-cube

Метамодель S-cube KB, представлена на рис. 2.3, описує основні компоненти цифрових промислових архітектур, їхні асоційовані атрибути, а також атаки та відмови, які, ймовірно, можуть статися на кожному компоненті.

В дослідженні [7] розширили підхід оцінки загроз, вразливостей та ризиків (TVRA) для інтегрованого аналізу ризиків безпеки та захищеності.

В дослідженні [8] ідентифікували технічні та соціотехнічні проблеми у спільному забезпеченні безпеки та захищеності для співпрацюючих промислових роботів (Cobots), проте не надали конкретних підходів до виявлення, аналізу та вирішення ризиків/конфліктів, пов'язаних із безпекою та захищеністю.

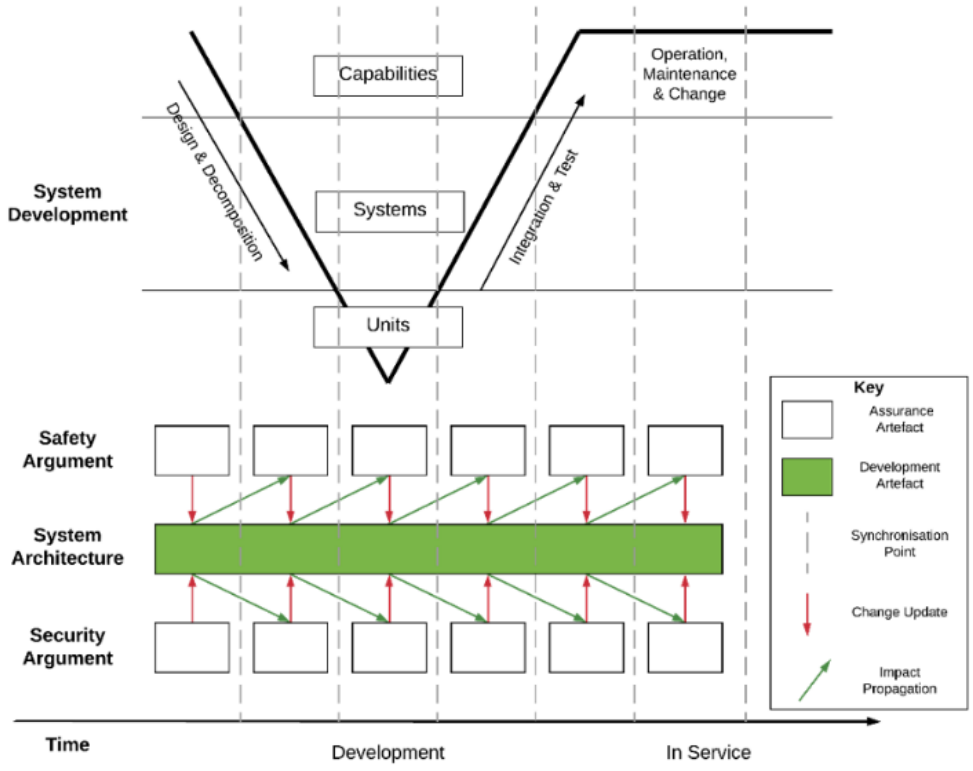


Рис. 2.4. Фреймворк забезпечення безпеки-захищеності (Safety-Security Assurance Framework, SSAF)

Рисунок 2.4 демонструє модель з фреймворку забезпечення безпеки-захищеності. Зокрема, він підкреслює процеси безпеки та захищеності, а

також їхню взаємодію протягом життєвого циклу системи. Кожен із етапів життєвого циклу системи висуває різні вимоги до фахівців із безпеки та захищеності: наприклад, ранні стадії зосереджені на сприянні інженерному процесу для зниження ризику системи, тоді як під час експлуатації увага фахівців зміщується на забезпечення очікуваного виконання операцій та недопущення порушення жодних гарантійних заяв, зроблених раніше.

Ключова ідея, що лежить в основі SSAF, — це концепція незалежного спільного забезпечення (independent co-assurance), яка дозволяє здійснювати роботу окремо, але вимагає точок синхронізації (synchronisation points), де відбувається обмін інформацією та приймаються компромісні (trade-off) рішення. Це дозволяє фахівцям використовувати спеціалізовану експертизу та забезпечувати прогрес у межах кожного домену, оскільки існує спільне розуміння того, яка інформація буде потрібна, а також де і коли її слід надати.

Існують різні режими взаємодії, які варіюються від "силосних" (silos) (характеризуються дуже невеликою кількістю точок синхронізації та обмеженою міждоменною комунікацією) до уніфікованих підходів (unified approaches) (де атрибути спільно проектуються та спільно забезпечуються). Необхідною передумовою для визначення інформаційних потреб у точках синхронізації є розуміння причинно-наслідкових зв'язків усередині доменів та між ними.

2.2.3. Проблема виявлення та вирішення конфліктів

Більшість досліджень у цій сфері зосереджувалися на спільному проектуванні вимог, приділяючи недостатню увагу методологіям виявлення та вирішення конфліктів, що виникають внаслідок інтеграції безпеки та захищеності.

В роботі [9] ідентифікували різні домени CPS, де можуть існувати конфлікти безпеки та захищеності, але обмежилися лише вказівками. Вони запропонували підхід до вирішення конфліктів безпеки через надання

багаторівневих або перекриваючих заходів безпеки та захищеності, проте цей метод може призвести до надмірності та/або додаткових конфліктів у системі. В [10] запропонували підхід для аналізу вимог безпеки та захищеності та вирішення конфліктів у ПСК, використовуючи оцінку ризиків на основі експертних знань. Цей метод може бути схильний до недооцінки впливу подій, що призводить до неоптимального ранжування ризиків. Крім того, він має обмежену застосовність до непов'язаних вимог або до фаз проектування та реалізації.

Інші споріднені дослідження були переважно зосереджені на автомобільній та авіаційній промисловості, приділяючи менше уваги ПСК.

Дана робота вирізняється тим, що вона виходить за межі фази аналізу вимог, охоплюючи фази проектування та реалізації системи. Це досягається через використання кейс-стаді, що відображає реальну ПСК.

2.3. Методологія аналізу та вирішення конфліктів безпеки та захищеності промислових систем керування та моніторингу технологічних процесів

У даній роботі запропоновано методологію, яка інтегрує методику системного теоретичного процес-аналізу (STPA-SafeSec) та підхід навчання на основі конфліктів (CDCL) з метою комплексного аналізу безпеки та захищеності, виявлення та розв'язання конфліктних вимог.

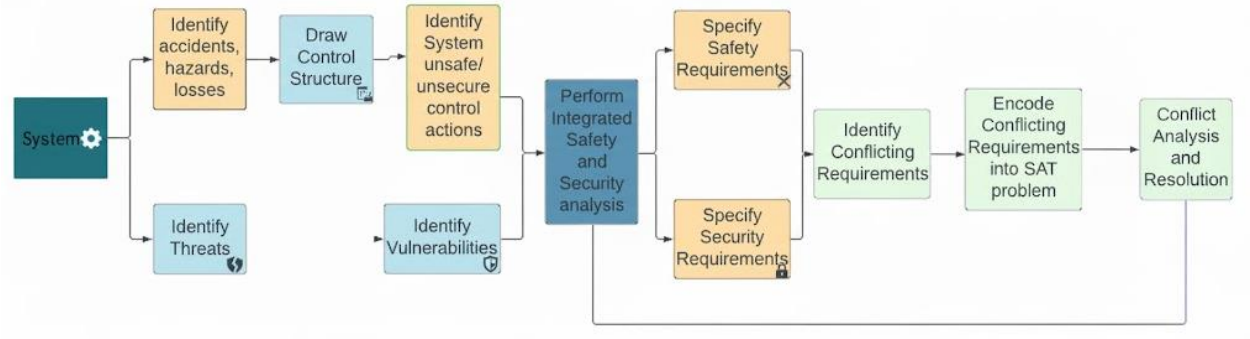


Рис. 2.5. Пропонована методологія

Ця методологія може бути застосована на етапах аналізу вимог, проектування системи або її реалізації.

2.3.1. Підхід до розробки методології

Методика STPA-SafeSec була розроблена на основі STPA та STPA-Sec для усунення недоліків цих попередніх підходів, які виконували аналіз безпеки та захищеності ізольовано. STPA-SafeSec забезпечує інтегрований аналіз безпеки та захищеності з позиції "зверху-вниз".

Метод ідентифікує як відмови компонентів, так і відмови взаємодії компонентів. Він також визначає вразливості захищеності та відповідні вимоги (наприклад, сценарії, що призводять до порушення обмежень захищеності та безпеки). Отримані результати використовуються для удосконалення концепції системи з метою підвищення її безпечності та захищеності. Крім того, STPA-SafeSec відображає причинно-наслідкові сценарії чи вразливості на потенційні втрати та сприяє розробці адекватних засобів контролю (обмежень) поведінки системи.

Запропонована методологія поєднує концепцію STPA-SafeSec та підхід CDCL для спільного проектування безпеки та захищеності, виявлення та розв'язання конфліктів. Ключовою перевагою цієї методології є її здатність враховувати та виявляти конфлікти, які можуть виникнути як внаслідок спільного проектування безпеки та захищеності, так і на етапах проектування та реалізації системи.

Методологія охоплює шість послідовних фаз. Перші три фази присвячені детальному аналізу безпеки, захищеності та їх інтеграції, а наступні фази включають виявлення, аналіз та вирішення конфліктів, а також визначення стратегій мінімізації ризиків.

1. Виконання глибокого аналізу безпеки (Safety)

Це початкова фаза методології. Вона передбачає аналіз структури керування системи для ідентифікації та визначення можливих дій керування та/або небезпечних дій керування. На цьому етапі експерти виявляють та

класифікують аварії або небезпеки, що можуть призвести до прийнятних чи неприйнятних втрат (як представлено у таблиці 2.1). Фаза дозволяє зіставити дії керування з компонентами чи змінними процесу, якими вони управляють.

Таблиця 2.1.

Перелік втрат і небезпек промислової системи

Втрати та небезпеки	**Референс**	**Посилається на**
Втрати (Losses)		
Втрата життя або травмування	[L-1]	
Втрата або пошкодження обладнання	[L-2]	
Втрата або пошкодження продукту	[L-3]	
Фінансові збитки	[L-4]	
Забруднення навколишнього середовища	[L-5]	
Небезпеки (Hazards)		
Експлуатація установки поза заданими параметрами (set points)	[H-1]	[L-1], [L-2], [L-3], [L-4], [L-5]
Нездатність установки підтримувати змінні процесу в межах визначеного порогу під час виробництва	[H-2]	[L-1], [L-2], [L-3], [L-4], [L-5]
Викид великого об'єму шкідливих речовин в установку	[H-3]	[L-1], [L-2], [L-3], [L-4], [L-5]
Одночасне відкриття клапанів випуску продукту та розвантаження установки	[H-4]	[L-1], [L-3], [L-4]
Установка випускає (викидає) забруднені матеріали	[H-5]	[L-1], [L-5]

2. Виконання глибокого аналізу захищеності (Security)

Дана фаза зосереджена на виявленні та класифікації системних загроз і вразливостей. Глибокий аналіз захищеності спрямований на ідентифікацію загроз, пов'язаних з конфіденційністю, цілісністю та доступністю системи. Фахівці з захищеності отримують необхідні знання про систему для виявлення слабких місць, що загрожують її захищеності. Прикладами загроз

є ін'єкція команд, маніпуляція командами, затримка або втрата команд, маніпуляція або втрата вимірювань.

3. Виконання інтегрованого аналізу безпеки та захищеності

На цьому етапі відбувається взаємодія між фахівцями з безпеки та захищеності для забезпечення того, що цілі захищеності посилюють безпеку і не підривають цілі безпеки, і навпаки. Ця фаза є критично важливою для забезпечення загальної безпечної та захищеної експлуатації ПСК. Вона оптимізує гармонізацію цілей безпеки та захищеності. Вимоги безпеки та захищеності визначаються на основі аварій, небезпек, втрат, причинних факторів, небезпечних дій керування, загроз та вразливостей, ідентифікованих у фазах 1 та 2.

4. Виявлення конфліктних вимог

Інтеграція аналізу безпеки та захищеності може призводити до конфліктів, відомих або невідомих фахівцям. Конфлікти можуть виникати як у межах окремих доменів (безпеки чи захищеності), так і на етапі їхньої інтеграції, а також можуть стосуватися конфлікту цілей проектування та цілей безпеки/захищеності.

Приклад конфлікту. Система А, розроблена для коректної роботи в умовах шуму, може зіткнутися з тим, що введення шуму в певному стані призводить до неконтрольованого збільшення чи зменшення змінних процесу, що конфліктує з обмеженнями безпеки/захищеності або нормативною поведінкою системи.

У цій фазі аналізуються всі можливі сценарії, що можуть призвести до конфлікту. Для виявлення конфліктів використовується метод, заснований на чотирьох принципах:

1) джерело контролера, що видає дії керування (SC),

2) тип дії керування (T) (надання або ненадання),

3) дія керування (CA),

4) контекст, у якому надається або не надається дія керування (Co).

Конфлікт виникає, коли надання або ненадання дії керування призводить до небезпек/загроз.

Приклад ADS. Розглянемо автоматичну систему дверей (ADS) у критичних спорудах (банки, аеропорти), призначену для виявлення зброї та автоматичного закриття дверей (вимога захищеності). Однак, під час надзвичайної ситуації (наприклад, пожежі), ADS повинна виконувати вимоги безпеки для цілей евакуації, тим самим компрометуючи цілі захищеності. У цьому випадку виконання або невиконання вимог призводить до небезпек/загроз.

5. Аналіз та вирішення конфліктів

Аналіз та вирішення конфліктів виконується, коли конфліктні вимоги виникають під час інтеграції або коли цілі проектування суперечать цілям безпеки/захищеності. Ця фаза дозволяє експертам визначити причинні фактори та розробити стратегії вирішення конфліктів. Отримані знання необхідні для перегляду обмежень безпеки та захищеності та/або цілей проектування системи. У нашій методології для аналізу та вирішення конфліктів використовується підхід CDCL.

6. Перевизначення обмежень безпеки та захищеності або стратегій пом'якшення

На завершальному етапі вимоги безпеки та захищеності, визначені у фазі 3, підлягають переоцінці з метою їхньої відповідності поточному стану системи, базуючись на знаннях, отриманих під час аналізу та вирішення конфліктів. Обмеження безпеки та захищеності перевизначаються для гарантування відсутності конфліктів. Також можуть бути визначені стратегії мінімізації ризиків для досягнення загальних цілей безпеки та захищеності системи.

2.3.2. Підхід системного процес-аналізу та захищеності

Методика STPA-SafeSec ґрунтується на фундаментальних принципах системного теоретичного процес-аналізу (STPA), розширюючи їх на домен

захищеності (Security). Підхід STPA-SafeSec нівелює слабкі сторони архітектур STPA та STPA-Sec, забезпечуючи взаємозалежність між обмеженнями захищеності та безпеки. Результати аналізу STPA-SafeSec допомагають експертам ідентифікувати потенційні небезпеки (аварії безпеки) або загрози (вразливості захищеності), які можуть спричинити системні втрати.

STPA-SafeSec пропонує уніфікований та інтегрований підхід, який надає рівноцінної важливості як безпеці, так і захищеності системи, що обґрунтовує його використання у даному дослідженні. В STPA-SafeSec обмеження безпеки та захищеності визначаються на основі структури керування системи. Крім того, аналіз STPA-SafeSec вимагає попереднього визначення втрат та небезпек, структури керування, загроз та/або вразливостей, а також обмежень безпеки та захищеності.

2.3.3. Підхід навчання на основі конфліктів

Метод навчання на основі конфліктів (CDCL) є еволюцією підходу DPLL, використовуючи стандартний алгоритм пошуку з поверненням (backtracking), де після кожного призначення рішення виконується одиничне поширення (unit propagation), формуючи новий рівень рішення.

Ключова перевага підходу CDCL полягає у використанні техніки нехронологічного повернення (non-chronological backtracking): повернення ініціюється одразу після виявлення конфлікту, а під час розв'язання конфлікту відбувається вивчення нових клауз (clause learning). CDCL здійснює "перестрибування" на відповідний рівень рішення, прийнятий до виникнення конфлікту.

Підхід CDCL оперує клаузами, представленими у кон'юнктивній нормальній формі (CNF). Клаузи складаються з літералів, де літерал — це змінна a або її заперечення ¬a. CNF являє собою кон'юнкцію диз'юнктивних клауз. Наприклад, для набору літералів a,b,¬a (які можуть набувати значень

true (1) або false (0)), диз'юнктивними клаузами є $(\neg a \vee b)$ та $(a \vee b)$. Відповідно, CNF матиме вигляд $(\neg a \vee b) \wedge (a \vee b)$.

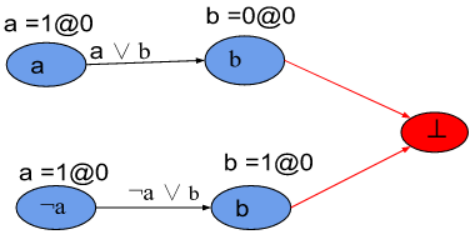
Визначення конфлікту. Розглянемо формулу CNF $\psi=(a \vee b) \wedge (\neg a \vee b)$ таку, що призначення a=true (1) та b=false (0) призводить до незадовільного результату (UNSAT). Конфлікт виникає, коли змінній a або b призначаються суперечливі значення в межах даної формули. Розв'язувач CDCL повертає результат UNSAT, якщо він не може вирішити конфлікт шляхом знаходження задовільного призначення, інакше повертає SAT.

Під час призначення змінних CDCL використовує концепцію одиничного поширення (Unit Propagation) або булевого обмеження поширення (BCP) для детермінування булевого значення, яке має бути призначене змінній для задоволення формули. Наприклад, якщо у формулі $\alpha=(a \vee b \vee c \vee d)$ змінним a, b та c призначено хибне значення (0), то за допомогою одиничного поширення CDCL присвоїть змінній d істинне значення (1) для задоволення α. Якщо клауза є одиничною, CDCL присвоїть змінній значення, яке робить клаузу задовільною.

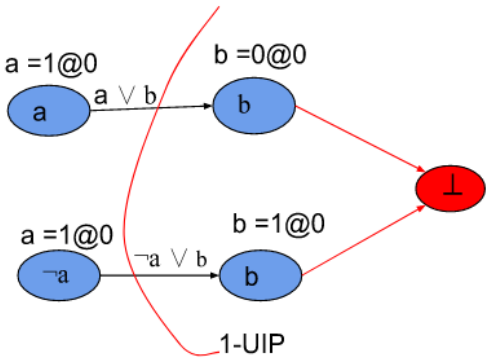
У разі виникнення конфлікту CDCL повертається до відповідного рівня рішення, прийнятого безпосередньо перед його виникненням.

Для аналізу та візуалізації призначень змінних, що спричинили конфлікт, створюються графіки наслідків (implication graphs). Це потужний інструмент, оскільки він дозволяє легко скасувати останнє рішення перед конфліктом, відмінити призначення та повторно призначити змінні до моменту розв'язання конфлікту.

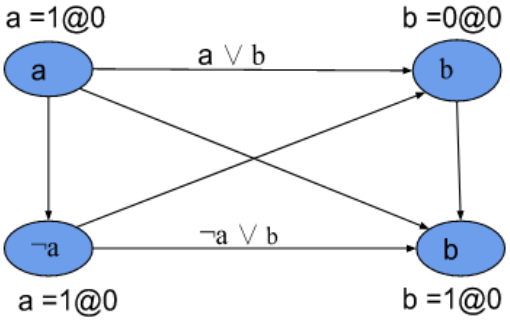
Під час повернення вивчаються нові клаузи. Сучасні розв'язувачі CDCL SAT реалізують концепцію першої унікальної точки наслідків (First Unique Implication Point, UIP) для навчання клауз. UIP представляє вузол або шлях, найближчий до конфліктного вузла в графі наслідків, і його використання необхідне для зменшення навчання надлишкових нових клауз.



а) Граф наслідків для ψ



б) Перша унікальна точка наслідків (First-UIP) для ψ



в) Граф розв'язання конфлікту для ψ

Рис. 2.6. Графи наслідків для аналізу та розв'язання конфлікту

Приклад аналізу конфлікту. Розглянемо клаузи C1=(a∨b) та C2 =(¬a∨b) у формулі ψ. Граф наслідків (рис. 2.6 а) для ψ показує, що призначення a=1 та b=0 на рівні рішення 0 робить C1 задовільною. Однак, якщо зберегти те саме призначення для C2, вона стає незадовільною, змушуючи ψ повернути UNSAT. Для задоволення ψ необхідно призначити b=1, що суперечить початковому призначенню b=0 і призводить до

конфлікту. CDCL повертається до рівня рішення 0 та скасовує призначення a. Під час повернення, як показано на рис. 2.6 б, перший UIP допомагає визначити коректний розріз для вузлів. Вивчена клауза C у цьому прикладі — це (a∨¬a). Ця нова клауза, звана клаузою конфлікту, додається до ψ для уникнення повторного призначення, що призводить до конфлікту. Під час розв'язання конфлікту (рис. 2.6 в) здійснюється перевизначення a=0 та b=1, що робить ψ задовільною.

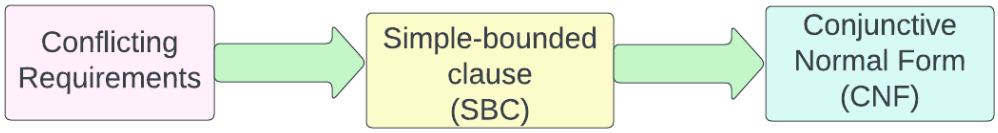


Рис. 2.7. Кодування конфліктних вимог у SAT задачу

Вимоги безпеки та захищеності в ПСК часто представлені як обмежені умови (constrained conditions), де змінні системи та процесу повинні знаходитися в межах заданого набору інтервалів, а не як булева формула чи CNF. Це створює проблему кодування конфліктних вимог у задачу SAT.

Для вирішення цієї проблеми пропонується метод (рис. 2.7) перетворення вимог безпеки або захищеності спочатку у просту обмежену клаузу (Simple Bounded Clause, SBC), а потім у CNF. Концепція SBC була застосована у різних галузях, включаючи стохастичні системи, нелінійні системи керування, машинне навчання та штучний інтелект. Кодування конфліктних вимог для обмежених умов було реалізовано мовою Python.

2.4. Приклад застосування пропонованої методології до технологічного процесу

Для демонстрації та валідації запропонованої методології було обрано процес який є симуляційною моделлю хімічного процесу, спеціально розробленою для досліджень у сфері промислових систем керування.

Вибір моделі обґрунтовано трьома основними факторами:

- Поширена модель яка є загальновизнаною моделлю для вивчення кібер-фізичних систем (CPS).

- Складність архітектури - модель містить різноманітні компоненти, рівні та змінні процесу, характерні для сучасних хімічних заводів: реактор, компресор, стрипер, конденсатор, сепаратор, аналізатори, датчики, виконавчі механізми (клапани), а також компоненти живлення, тиску та температури.

- Релевантність для безпеки/захищеності - модель активно використовується для дослідження безпеки CPS та ідентифікації векторів атак.

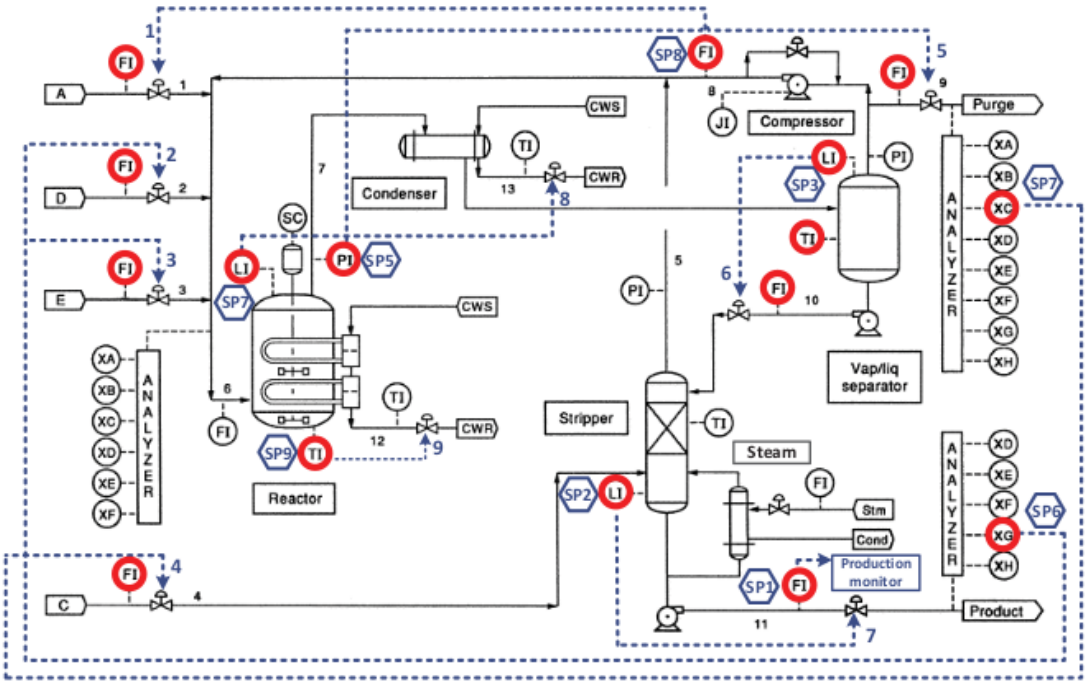


Рис. 2.8. Модель технологічного процесу

Завод містить вісім хімічних компонентів: чотири реагенти (A, C, D та E), два рідкі продукти, один побічний продукт та один інертний компонент. Хімічні реакції описуються наступними рівняннями:

$$A(g)+C(g)+D(g)\rightarrow G(\text{рідина})\Rightarrow \text{Продукт 1}$$

$$A(g)+C(g)+E(g)\rightarrow H(\text{рідина})\Rightarrow \text{Продукт 2}$$

У поточному дослідженні запропонована методологія застосована до системи керування хімічним реактором (CRCS) заводу. Хімічний реактор є центральною одиницею заводу, де відбуваються реакції для синтезу продуктів G та H.

Фаза 1. Глибокий аналіз безпеки (Safety Analysis)

Відповідно до методології, перша фаза передбачає проведення глибокого аналізу безпеки системи CRCS для ідентифікації втрат та небезпек на системному рівні, які представлені у таблиці 2.1.

Наступним кроком є вивчення структури керування (control structure) для отримання детального переліку команд, керованих змінних процесу (MPV) та зворотного зв'язку під час хімічного виробництва.

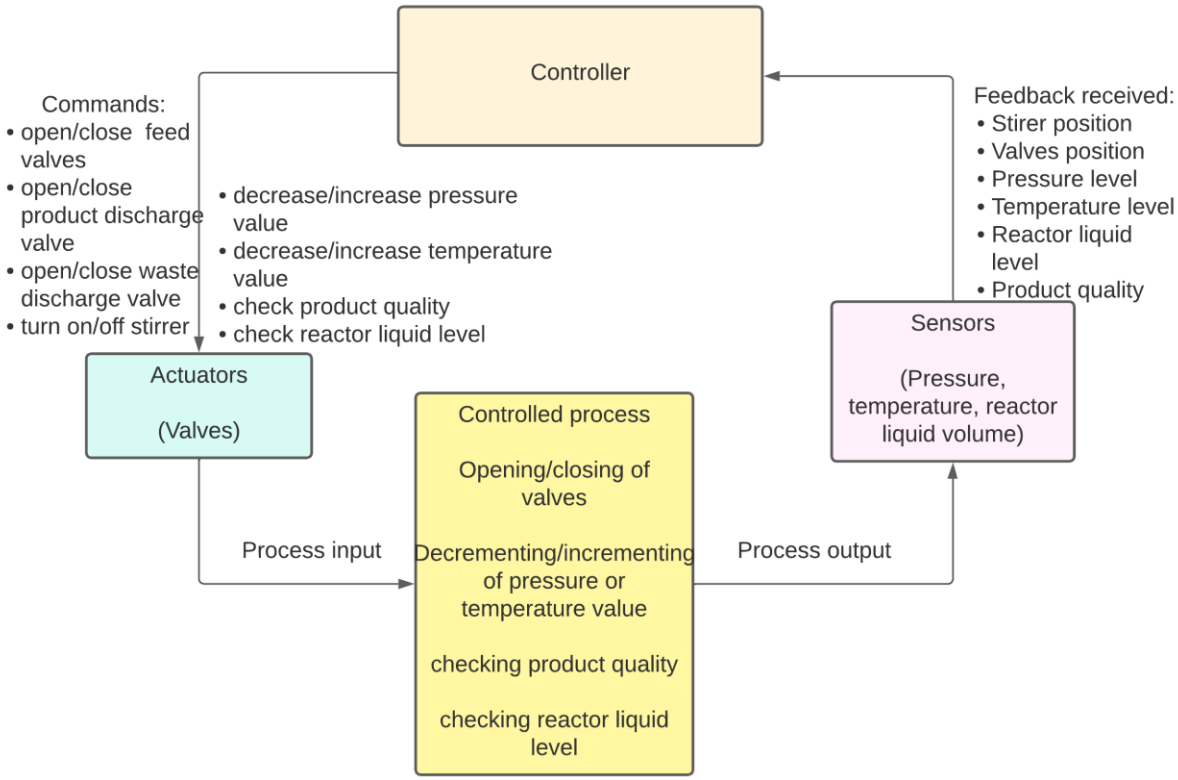


Рис. 2.9. Система керування та моніторингу технологічного процесу

Цілі та завдання системи керування процесом, включають:

1) підтримку змінних процесу в межах бажаних значень;

2) забезпечення роботи процесів у межах обмежень обладнання;

3) зменшення коливань швидкості продукту та змінних процесу під час збурень;

4) мінімізацію руху клапанів, що впливає на інші процеси;

5) швидке й плавне відновлення після збурень, зміни суміші продукту або швидкості виробництва.

Ми здійснюємо аналіз системи для визначення необхідних дій керування та небезпечних дій керування, які можуть спричинити небезпеки, що призводять до втрат. Для визначення цих дій застосовуються чотири способи, як показано у таблиці 2.2.

Таблиця 2.2.

Дії керування та їхній вплив на систему

Дія Керування (CA)	**Небезпечні дії керування (UCA)**
CA-1: Обладнання має працювати в межах заданого діапазону.	**Надана небезпечно:** Нездатність контролювати операції реактора в межах встановлених обмежень призводить до зупинки або пошкодження обладнання.
Надана надто рано/пізно: Примусове дотримання роботи обладнання в межах заданого діапазону, але надто пізно, викликає пошкодження обладнання або знос.	
Припинена надто рано/пізно: Зупинка надто пізно, коли обладнання працює поза межами, викликає пошкодження.	
CA-2: Підтримка змінних процесу в межах бажаних значень.	**Надана небезпечно:** Призводить до зупинки або пошкодження обладнання або продукту.
Надана надто рано/пізно: Надто пізно викликає зупинку обладнання/пошкодження або пошкодження продукту.	
CA-3: Мінімізація частих рухів клапанів.	**Надана небезпечно:** Велике вивільнення сировини в реактор викликає переповнення реактора або пошкодження продукту.

Дія Керування (CA)	Небезпечні дії керування (UCA)
Не надана: Відкриття клапанів продукту та відходів одночасно викликає переповнення реактора або пошкодження продукту.	
Надана надто рано/пізно: Закриття клапанів живлення або скидання надто рано/пізно впливає на якість продукту.	
Припинена надто рано/пізно: Відкриття/закриття клапанів живлення надто довго/рано впливає на якість продукту.	
CA-4: Зменшення коливань швидкості живлення під час збурень.	**Надана небезпечно:** Викликає зупинку системи або пошкодження продукту.
Надана надто рано/пізно: Надто пізно призводить до пошкодження продукту.	
Припинена надто рано/пізно: Припинення надто рано/пізно призводить до зупинки або пошкодження продукту.	
CA-5: Завод повинен швидко та плавно відновлюватися після збурень та змін швидкості виробництва.	**Надана небезпечно:** Зупинка системи, пошкодження обладнання або продукту.
Надана надто рано/пізно: Надто пізно призводить до зупинки системи, пошкодження обладнання або продукту.	
Припинена надто рано/пізно: Припинення надто рано/пізно призводить до зупинки системи, пошкодження обладнання або продукту.	

2.4.1. Вимоги безпеки

На основі аналізу, представленого в таблиці 2.2, ми можемо вивести небезпечні дії керування (UCA) та їхні причинні сценарії (CS) для кожної дії керування (CA):

CA-1: Обладнання має працювати в межах заданого діапазону.

UCA-1: Обладнання працює за межами встановлених обмежень.

CS-1: Контролер не здатний регулювати роботу заводу в межах заданого діапазону.

CA-2: Підтримка змінних процесу в межах бажаних значень.

UCA-2: Робота заводу за межами змінних процесу.

CS-2.1: Відмова датчиків правильно моніторити поточний стан системи.

CS-2.2: Відсутність зв'язку між датчиком та контролером.

CA-3: Мінімізація частих рухів клапанів.

UCA-3: Відкриття/закриття клапанів без обмежень.

CS-3.1: Контролер видає команду, яка викликає одночасне відкриття клапанів продукту та відходів через поганий зворотний зв'язок від датчика.

CS-3.2: Відмова датчика передавати поточний стан клапанів.

CS-3.3: Відмова виконавчого механізму отримувати команди від контролера.

CA-4: Зменшення коливань швидкості живлення під час збурень.

UCA-4: Активація збурень, що збільшують швидкість живлення.

CS-4: Нездатність системи керування стабілізувати швидкість живлення під час збурень через відмову або атаку.

CA-5: Завод повинен швидко та плавно відновлюватися після збурень.

UCA-5: Завод не відновлюється після збурень.

CS-5: Збільшення змінної процесу під час збурень, що призводить до зупинки заводу.

2.4.2. Вимоги захищеності

Проведення детального аналізу безпеки дозволяє перейти до фази аналізу захищеності, який ґрунтується на загрозах кібербезпеки (SCT) та вразливостях цільової системи. У системі ідентифіковано різні загрози, класифіковані за тріадою CIA (Confidentiality, Integrity, Availability).

1) Загрози конфіденційності (Confidentiality)

SCT-C-1: Несанкціонований доступ до власних даних заводу.

Сценарії/Атаки: Зовнішня особа або невдоволений співробітник отримує доступ до операційних даних заводу для подальшої експлуатації.

SCT-C-2: Несанкціонований доступ до HMI або команд керування.

Сценарії/Атаки: Віддалений доступ до HMI або команд керування зловмисником з метою маніпуляції системою.

2) Загрози цілісності (Integrity)

SCT-I-1: Маніпуляція командами.

Сценарії/Атаки: Віддалений доступ до контролера або HMI для ін'єкції або модифікації команд керування.

SCT-I-2: Втрата команд.

Сценарії/Атаки: Атака "людина посередині" (MITM), що призводить до втрати команд керування.

SCT-I-3: Маніпуляція вимірюваннями.

Сценарії/Атаки: Атака MITM, яка перехоплює та модифікує вимірювання датчиків, підставляючи фальшиві значення.

SCT-I-4: Втрата вимірювань.

Сценарії/Атаки: Атака "людина посередині" (MITM), що призводить до втрати вимірювань датчиків.

3) Загрози доступності (Availability)

SCT-A-1: Затримка команд.

Сценарії/Атаки: Атака "відмова в обслуговуванні" (DOS), яка визначає оптимальний час для затримки команд керування, тим самим переводячи завод у небезпечний стан.

SCT-A-2: Затримка вимірювань.

Сценарії/Атаки: Атака DOS, яка затримує вимірювання датчиків, внаслідок чого контролер використовує застарілі дані з пам'яті, що не відображають поточний стан заводу для прийняття рішень.

2.4.3. Проектування безпеки та захищеності

Безпека та захищеність є двома фундаментальними властивостями ПСК, і їхня інтеграція набуває критичного значення. Інтеграція аналізу

безпеки та захищеності є необхідною умовою для забезпечення того, що цілі захищеності посилюють безпеку, а не підривають її, і навпаки.

При інтеграції результатів фаз 1 та 2 (аналіз безпеки та захищеності) виявляється, що небезпечні дії керування та їхні причинні сценарії у домені безпеки часто є синонімічними ідентифікованим загрозам у домені захищеності. Ця фаза усуває розрив, що виникає при ізольованому виконанні аналізу. Фахівці обох доменів співпрацюють для забезпечення загальної безпечної та захищеної роботи системи.

Фахівці із захищеності зіставляють загрози з можливими UCA та їхніми причинами для забезпечення повного охоплення всіх потенційних системних загроз. Фахівці із захищеності також переоцінюють систему з погляду безпеки, і навпаки.

У даній роботі ми зосереджуємося на вимогах безпеки заводу, які представлені у формі обмежених умов (constrained conditions). У таблиці 2.3 підсумовано визначені межі безпеки.

Таблиця 2.3.

Обмеження безпеки заводу

Компонент	**Межа (%)**	**Компонент**	**Межа**
Живлення A	[24, 30]	Тиск реактора (kPa)	[2800, 3000]
Живлення C	[60, 62]	Рівень стрипера (%)	[46, 54]
Живлення D	[62, 64]	Рівень реактора (%)	[54, 55]
Живлення E	[52, 55]	Якість (%)	[54, 55]
Продукт G	[52, 56]	Ціна (%)	[100, 120]
Продукт H	[42, 46]	Виробництво (%)	[22, 23]

Визначення вимог безпеки в ПСК як обмежених умов є суворим підходом до визначення меж, що є важливим для швидкої ідентифікації

порушень меж у доменах безпеки та захищеності. Наприклад, межа $A \in [25,30]$ є більш жорсткою та інформативною, ніж $A \in [0,30]$. Порушення або конфлікт виникає, коли дії або події змушують систему функціонувати поза встановленими межами. У випадку заводу система керування запроектована таким чином, щоб забезпечувати роботу в межах заданих точок; наприклад, завод автоматично зупиняється, коли тиск реактора перевищує 3000 кПа.

Тоді як безпека запобігає відмовам, захищеність захищає систему від атак. Деякі дослідження продемонстрували вплив атак типу відмова в обслуговуванні (DOS) або атак, спрямованих на порушення цілісності, на завод та успішність їх реалізації. На основі нашого аналізу визначено наступні вимоги захищеності для усунення всіх ідентифікованих загроз:

1) Вимоги конфіденційності (SC-C)

SC-C-1: До HMI (Human-Machine Interface) повинні мати доступ лише авторизовані користувачі з використанням надійних паролів та багатофакторної аутентифікації. Необхідно налаштувати інструменти безпеки та системи моніторингу для запобігання несанкціонованим спробам входу.

SC-C-2: Власні дані заводу повинні бути зашифровані для запобігання несанкціонованому ознайомленню з операційними командами та можливостями заводу.

2) Вимоги цілісності (SC-I)

SC-I-1: Кожен вхідний сигнал від HMI або контролера повинен проходити верифікацію.

SC-I-2: Система повинна визначати еталонний середній час для зв'язку між контролером, датчиками та виконавчими механізмами та навпаки.

SC-I-3: Необхідно створити захисний механізм для запобігання атакам, які модифікують команди керування, значення датчиків, виконавчих механізмів або швидкості живлення.

SC-I-4: Кожен користувач повинен бути аутентифікований перед доступом до об'єктів або систем заводу.

3) Вимоги доступності (SC-A)

SC-A-1: Необхідно здійснювати моніторинг мережевого трафіку процесу для виявлення аномальних патернів трафіку або незвичних затримок зв'язку між контролером та датчиками/виконавчими механізмами.

SC-A-2: Мережа заводу повинна бути стійкою до атак DOS шляхом встановлення брандмауерів та розподіленого розміщення серверів у різних дата-центрах.

Інтеграція аналізу безпеки та захищеності може призводити до конфліктних вимог. На основі прийнятого методу виявлення конфліктів, застосованого у нашому кейс-стаді, було встановлено, що активація деяких збурень конфліктує з межами безпеки/захищеності та типовою поведінкою системи. Зокрема, надання або ненадання CA-4 призводить до небезпек/ загроз при активації збурень, оскільки контролер виявився нездатним підтримувати змінні процесу та коливання швидкості живлення в межах прийнятного порогу, що суперечить цілям безпеки та захищеності заводу.

2.4.4. Аналіз та вирішення конфліктів в технологічному процесі

Введення збурень у хімічні заводи, зокрема в дану модель, піддає систему впливу шуму та коливань. Відповідно до цілей керування, завод спроектований для роботи в умовах збурень без помітного впливу на процеси чи змінні. Інколи таке проектування здійснюється для демонстрації надійності, стійкості та живучості системи, але воно може спричинити надмірність та порушення (конфлікти) системних властивостей. Аналіз роботи заводу в умовах збурень виявив наявність такої надмірності та порушень.

З нашого аналізу встановлено, що активація деяких збурень порушує безпеку та нормативну поведінку заводу. Для демонстрації цього впливу було використано код заводу у середовищі MATLAB.

Базова симуляція спочатку була проведена без активації збурень, використовуючи базові значення, що підтвердило нормативну поведінку (таблиця 2.3).

Використовуючи ті самі налаштування, були проведені симуляції з активацією збурень IDV(1) (ступінчасте збурення, що маніпулює співвідношеннями живлення A та C), IDV(11) (випадкове збурення, що впливає на температуру входу охолоджувальної води реактора) та IDV(13) (повільне дрейфове збурення, що впливає на кінетику реакції).

Результати симуляції показали, що активація збурень конфліктує з цілями безпеки та захищеності, спричиняючи аномальну поведінку заводу. Було зафіксовано:

- Зростання вартості виробництва більш ніж на 150% вище нормативних значень.

- Значне зниження швидкості виробництва та значне збільшення швидкості живлення.

- Рівні тиску реактора та стрипера продемонстрували високі та низькі пікові рівні відповідно, що призвело до зупинки заводу.

У таблиці 2.4 підсумовано вплив активації збурень на системні параметри (дані з трьох різних симуляцій зі збуреннями).

Таблиця 2.4.

Виробництво заводу під час активації збурень (зведена)

Компонент	**Симуляція 1 (діапазон)**	**Симуляція 2 (діапазон)**	**Симуляція 3 (діапазон)**
Живлення A	[28, 100]	[28, 100]	[10, 45]
Живлення C	[55, 61]	[57, 61]	[60, 63]
Живлення D	[62, 64]	[63, 64]	[63, 64]
Живлення E	[52, 55]	[53, 60]	[52, 56]
Продукт G	[52, 56]	[54, 58]	[54, 58]
Продукт H	[42, 46]	[37, 44]	[37, 44]
Тиск реактора	[2760, 2820]	[2780, 2960]	[2500, 2900]

Компонент	Симуляція 1 (діапазон)	Симуляція 2 (діапазон)	Симуляція 3 (діапазон)
Рівень стрипера	[30, 70]	[-30, 50]	[10, 80]
Рівень реактора	[62, 68]	[64, 69]	[64, 69]
Якість	[54, 55]	[54, 58]	[50, 57]
Ціна	[50, 250]	[50, 300]	[40, 300]
Виробництво	[22, 23]	[20, 23]	[20, 22]

Такі значні коливання можуть мати катастрофічні наслідки на хімічних, ядерних або водоочисних заводах.

Для аналізу конфліктних меж безпеки та захищеності, виявлених у таблиці 2.4, застосовано метод кодування, описаний у нашій методології.

Обмеження спочатку кодуються у просту обмежену клаузу (SBC), а потім перетворюються на CNF-формулу, придатну для розв'язання підходом CDCL.

Формалізація доменів:

D0: Домен загальних хімічних реакцій у реакторі TE.

D1: Піддомен реакцій, що виробляють Продукт G за нормальної роботи (без збурень): D1=A(g)+C(g)+D(g)=G(рідина).

D2: Піддомен реакцій, що виробляють Продукт H за нормальної роботи: D2=A(g)+C(g)+E(g)=H(рідина).

D3: Піддомен реакцій, що виробляють Продукт G під впливом збурень: D3=¬A(g)+¬C(g)+¬D(g)=¬G(g).

D4: Піддомен реакцій, що виробляють Продукт H під впливом збурень: D4=¬A(g)+¬C(g)+¬E(g)=¬H(g).

Заперечення компонента (¬) означає, що нижня або верхня межа компонента (або обидві) виходить за межі прийнятних безпекових порогів.

Вводимо булеві змінні для представлення обмежених властивостей безпеки:

l_1, l_3, l_5, l_7 — нижні обмежені властивості безпеки.

l_2, l_4, l_6, l_8 — верхні обмежені властивості безпеки.

Наприклад, $l_1 \leftrightarrow (a \geq 24)$, $l_2 \leftrightarrow (a \leq 30)$.

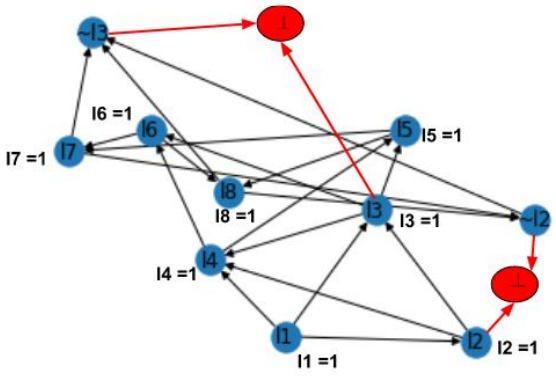
Формула CNF:

$$D_1 = (l_1 \wedge l_2) \vee (l_3 \wedge l_4) \vee (l_5 \wedge l_6)$$
$$D_2 = (l_1 \wedge l_2) \vee (l_3 \wedge l_4) \vee (l_7 \wedge l_8)$$
$$D_3 = (l_1 \wedge \neg l_2) \vee (\neg l_3 \wedge l_4) \vee (l_5 \wedge l_6)$$
$$D_4 = (l_1 \wedge \neg l_2) \vee (\neg l_3 \wedge l_4) \vee (l_7 \wedge \neg l_8)$$

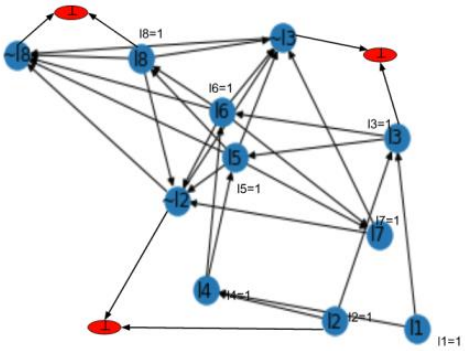
Таким чином, загальний домен, що включає конфлікти, може бути виражений як

$$D_0 = (D_1 \vee D_2) \wedge (D_3 \vee D_4) \equiv (D_1 \wedge D_3) \vee (D_2 \wedge D_4).$$

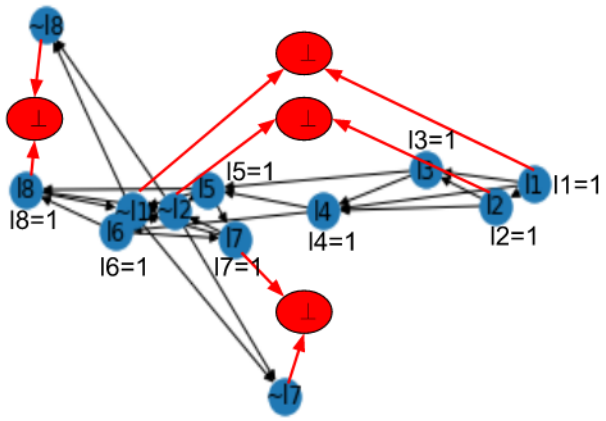
Ця формула D_0 передається скрипту на Python, який здійснює її перетворення у формулу CNF, придатну для обробки CDCL.



а) Граф наслідків для IDV(1)



б) Граф наслідків для IDV(11)



в) Граф наслідків для IDV(13)

Рис. 2.10. Процес аналізу та вирішення конфліктів

Під час аналізу конфліктів використовується граф наслідків. Для ідентифікації конфліктних меж на графі наслідків вони позначаються червоним кольором.

Істинне значення (True) змінній l_i призначається, якщо відповідна нижня чи верхня межа знаходиться в межах безпеки; інакше – хибне (False). Це призначення базується на знаннях про базову систему. Конфліктна межа виникає, коли змінна, що представляє межу, стає істинною і хибною в одному домені (що відображається графом наслідків).

Приклад. Граф наслідків чітко показує, що змінна l2 (верхня межа кількості живлення A) порушується: замість того, щоб бути ≤ 30%, вона зростає до 100% при активації IDV(1), IDV(11) та IDV(13), що призводить до конфлікту.

На фазі аналізу та вирішення конфліктів граф наслідків є критично важливим інструментом, який допомагає фахівцям (з безпеки/захищеності та проектування) точно визначити, яка змінна виходить за межі під час активації збурень.

Отже, запропонована методологія забезпечує інтегрований підхід до аналізу безпеки (safety) та захищеності (security), а також до виявлення та розв'язання конфліктів. Цей підхід досягається шляхом синергетичної

інтеграції методики STPA-SafeSec та алгоритму навчання на основі конфліктів (CDCL). Для демонстрації практичної застосовності методології її було успішно застосовано до моделі технологічного процесу заводу. Ключовою перевагою нашого підходу є його здатність виходити за межі виключно фази аналізу вимог.

Методологія може бути ефективно застосована на ранніх етапах проектування та розробки системи з метою превентивного підвищення її надійності, стійкості та живучості.

Висновки до розділу

Другий розділ присвячено розробленню ІТ-моделей і методології проєктування промислових систем керування, орієнтованих на забезпечення їхньої безпеки та захищеності.

Здійснено порівняльний аналіз сучасних підходів до інтеграції вимог безпеки і захищеності. Виявлено, що існуючі стандарти мають фрагментарний характер, що призводить до конфліктів між технічними та організаційними аспектами безпеки. Запропоновано методологію аналізу та вирішення конфліктів безпеки та захищеності, яка базується на принципах системного процес-аналізу та конфліктного навчання.

У межах цієї методології розроблено три ключові підходи:

- Системний процес-аналіз, який дозволяє визначати критичні точки взаємодії між підсистемами безпеки і захисту;

- Інтегрований аналіз ризиків, що уможливлює кількісну оцінку впливу кіберінцидентів на функціональну безпеку системи;

- Підхід навчання на основі конфліктів, який використовує зворотний зв’язок від попередніх інцидентів для адаптації моделей безпеки.

Розроблену методологію апробовано на прикладі конкретного технологічного процесу промислового підприємства. Проведено ідентифікацію вимог безпеки, моделювання архітектури захисту та аналіз

конфліктних взаємодій. Результати підтвердили можливість зниження ймовірності критичних відмов і покращення загальної стійкості системи керування технологічним процесом.

РОЗДІЛ 3. ІМПЛЕМЕНТАЦІЯ ІТ МОДЕЛЕЙ ТА МЕТОДОЛОГІЇ ОЦІНКИ РИЗИКІВ КІБЕРБЕЗПЕКИ ПРОМИСЛОВИХ СИСТЕМ КЕРУВАННЯ

3.1. Оцінка ризиків кібербезпеки промислових систем

Безпека критичної інфраструктури (КІ) та промислових систем постає як гострий виклик для національних та державних структур, що зумовлено зростанням складності, взаємозв'язку цих систем та їхнім віддаленим управлінням. Забезпечення стійкості КІ вимагає інженерного аналізу кібербезпеки та пов'язаних ризиків, які можуть бути використані зловмисниками для ініціювання високонаслідкових подій (HCE). Такі події здатні спричинити катастрофічні наслідки, включаючи пошкодження обладнання, екологічне забруднення (довкілля/водопостачання), значні фінансові збитки або навіть людські жертви.

Ключовим завданням є ідентифікація та пріоритизація таких дій або атак, які можуть призвести до HCE, що паралізують критичні функції організації. У цьому дослідженні ми пропонуємо підхід до оцінки ризиків кібербезпеки, що поєднує методику кіберінформованого інжинірингу, орієнтованого на наслідки (Consequence-Driven Cyber-Informed Engineering, CCE) та байєсову мережу переконань (Bayesian Belief Network, BBN), доповнену аналізом чутливості (Sensitivity Analysis, SA). Для доказу концепції (Proof of Concept) запропонований підхід було протестовано на моделі технологічного процесу, що дозволило ефективно виявити та пріоритизувати ефекти доміно, спричинені атаками, які імітують завади або шум у КІ.

Забезпечення безпеки КІ вимагає глибокого розуміння середовища операційних технологій (ОТ), його складності та взаємозв'язку. Історично КІ створювалася для локального керування, однак сучасні системи керуються та

контролюються з віддалених місць, що істотно підвищує їхню вразливість до кібератак.

Для захисту критичних активів необхідно аналізувати ризики та загрози кібербезпеки, а також їхній потенційний вплив на процеси та системи. Сучасні кіберзагрози постійно зростають, а зловмисники використовують складні інструменти для обходу механізмів безпеки та здійснення кіберсаботажу. Незважаючи на це, багато організацій помилково вважають свої системи захищеними, не виділяючи достатнього фінансування та ресурсів на впровадження актуальних практик кібербезпеки. Оскільки повне усунення всіх можливих кіберризиків є неможливим, критично важливим є визначення та фокусування на діях, які можуть призвести до високонаслідкових подій (HCE).

У сфері IT: HCE — це події, які впливають на критичні функції організації, паралізуючи її повсякденну діяльність. У критичних системах HCE мають катастрофічний вплив на КІ (енергетика, ядерні станції, водоочищення), викликаючи пошкодження обладнання/зупинку заводу, забруднення навколишнього середовища, фінансові втрати, травми або смерть. HCE представляють події з найбільш серйозним кумулятивним впливом на систему.

Було розроблено низку інструментів (таких як аналіз дерева несправностей (FTA), дерева атак, фреймворк кібербезпеки NIST) для запобігання кіберризикам. Хоча ці методики ефективні для виявлення вразливостей та загроз, вони недостатньо здатні ідентифікувати HCE на ранніх етапах проектування та розробки систем. Виявлення HCE на ранніх стадіях є ключовим для запобігання кіберризикам, що загрожують національній безпеці.

З метою усунення цієї слабкості було запропоновано підхід CCE, що є фреймворком, що сприяє залученню інженерного персоналу до розуміння та пом'якшення високонаслідкових кіберзагроз, які постійно еволюціонують.

CCE є підходом "зверху-вниз", який зосереджується на:

- Виявленні НСЕ, що впливають на КІ.

- Аналізі способів, якими зловмисник може експлуатувати систему для спричинення НСЕ.

- Розробці цільових стратегій пом'якшення.

Історично НСЕ спричинялися різноманітними атаками (фішинг, DDoS, вимагачі, маніпуляції даними). Особливо важливим є випадок атаки 2021 року на систему SCADA об'єкта водопостачання Каліфорнії та кібератака на німецький металургійний завод, що призвела до пошкодження печі.

Наш підхід долає основні слабкості попередніх робіт, а саме — високу залежність від людських або експертних знань під час пріоритизації НСЕ. BBN-SA надає вимірювані результати та оцінки, що ґрунтуються на даних симуляції системи.

Наш підхід має дві основні складові:

- Аналіз та пріоритизація наслідків (Фаза CCE) - включає аналіз, виявлення та пріоритизацію НСЕ.

- Цільовий аналіз на основі наслідків (фаза BBN-SA) - включає аналіз загроз безпеки та демонстрацію того, як кіберзловмисники можуть ініціювати виявлені НСЕ.

В основі методології лежить виявлення каскадних ефектів, спричинених порушенням КІ. Фаза BBN-SA моделює вплив збою, спричиненого завадами, розкриваючи критичність окремих компонентів/процесів для функціонування всієї системи.

3.2. Інтегрована методологія для пріоритизації подій при керуванні та моніторингу технологічних процесів

У даній роботі запропоновано методологію, що інтегрує кіберінформований інжиніринг, орієнтований на наслідки (CCE) та Байєсову мережу переконань (BBN) з аналізом чутливості (SA). Мета полягає в аналізі, виявленні та пріоритизації високонаслідкових подій (НСЕ), здатних

паралізувати критичну інфраструктуру, таку як енергетичні, ядерні або водоочисні станції.

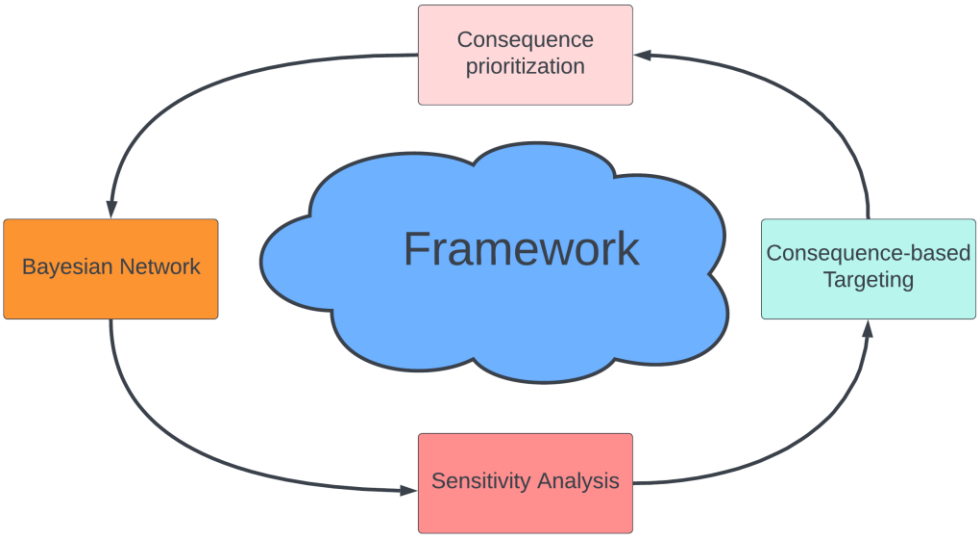


Рис. 3.1. Структура пропонованого фреймворку

3.2.1. Кіберінформований інжиніринг та Байєсова мережа переконань

Дана методологія є удосконаленою методологією сфокусованою на виявленні НСЕ з найгіршими функціональними наслідками для КІ.

Призначення ССЕ: надає організаціям необхідні етапи для забезпечення захисту активів, що виконують найкритичніші функції.

Оцінка ризиків: ССЕ дозволяє адекватно ідентифікувати та кількісно оцінювати ризики кібербезпеки, спричинені конкретними кіберзловмисниками, та формувати розуміння потенційного кібернетичного та фізичного впливу кіберподії.

Байєсова мережа переконань (BBN) — це графова модель, яка відображає ймовірнісні взаємозв'язки між множиною змінних, слугуючи інструментом штучного інтелекту для моделювання невизначеності в системі. Являє собою орієнтований ациклічний граф (DAG), де вузли відповідають змінним, а дуги (ребра) — причинно-наслідковим зв'язкам. Моделює ймовірнісне виникнення подій за наявності невизначеності.

Важливою особливістю є виявлення критичних змінних з урахуванням інших впливових факторів.

Аналіз чутливості (SA) використовується для валідації моделі BBN шляхом ідентифікації найбільш критичних параметрів, коригування яких значно впливає на загальний результат BBN. SA вимірює, як зміни у вхідних змінних впливають на вихідну змінну, підвищуючи коректність та надійність моделі.

3.2.2. Структура запропонованої методології

Запропонована структура складається з двох основних фаз:

Фаза 1 (пріоритизація наслідків) - аналіз, виявлення та кількісна пріоритизація HCE за допомогою моделей BBN та SA.

Фаза 2 (Цільовий аналіз на основі наслідків) - дослідження загроз безпеки та сценаріїв, за допомогою яких кіберзловмисник може використати систему для спричинення виявлених HCE.

Фаза пріоритизації наслідків - є критичною, оскільки від її результатів залежать подальші етапи. На цій фазі визначаються найгірші сценарії, події або атаки, що можуть призвести до HCE, шляхом визначення граничних умов та критеріїв тяжкості для оцінки прийнятних/неприйнятних ризиків.

Для ідентифікації HCE прийнято таксономію функцій CCE для виявлення критичних компонентів та функцій (наприклад, виробництво сутності або бізнес-функції), порушення яких є необхідним для спричинення HCE.

Моделювання BBN складається з двох компонентів:

1. Граф мережі (якісний аналіз): орієнтований ациклічний граф (DAG), що відображає залежності між вузлами (змінними).

2. Таблиця умовних імовірностей (CPT) (кількісний аналіз): Представляє умовні ймовірності вузла відносно його батьків.

У даному дослідженні, щоб мінімізувати залежність від експертних знань, CPT побудована на основі даних симуляції системи. BBN

використовується для обчислення апостеріорних ймовірностей (наприклад, $P(I|A_1)$ — ймовірність впливу на цілісність I за умови атаки A_1) відповідно до теореми Байєса:

$$P(I \mid A_1) = \frac{P(A_1 \mid I)P(I)}{P(A_1 \mid I)P(I) + P(A_1 \mid \neg I)P(\neg I)}$$

Аналіз чутливості (SA) застосовується для визначення чутливості кожного вузла до цільового вузла, вимірюючи, як зміни вхідних змінних впливають на вихід. SA допомагає ідентифікувати критичні вхідні змінні, що є життєво важливим для прийняття рішень та підвищення надійності моделі BBN. SA реалізовано за допомогою GeNIe Bayesian Modeler.

Моделювання в BBN відображає причинно-наслідковий зв'язок між вузлом атаки A_k та критеріями SIAC (як показано на рис. 3.2).

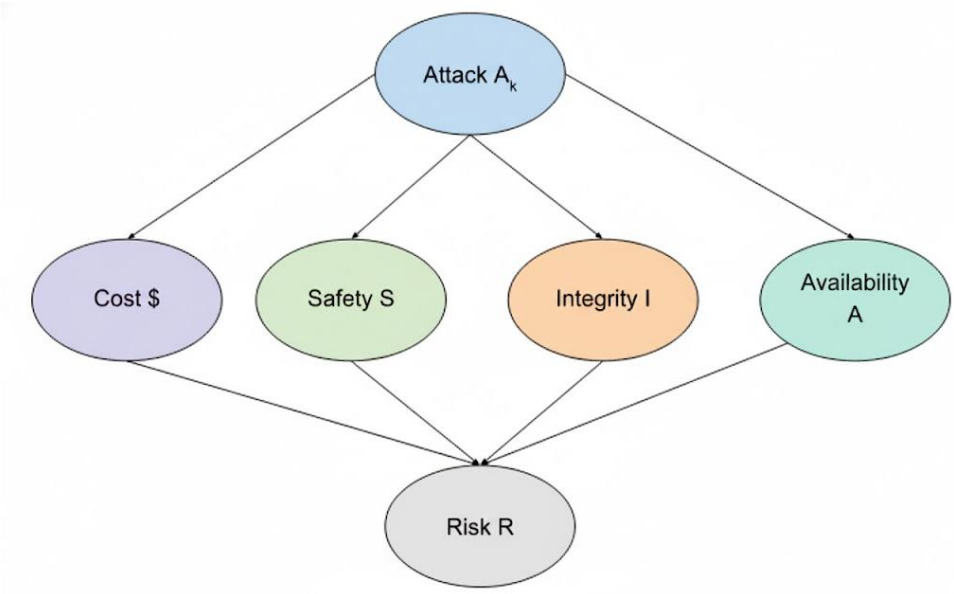


Рис. 3.2. Граф засобами BBN

Фаза цільового аналізу на основі наслідків вимагає від експертів мислення з позиції зловмисника, досліджуючи, як можна порушити систему для ініціювання НСЕ. Аналізуються всі потенційні слабкі місця: шлюзи,

центри обробки даних, мережеві компоненти та, особливо, люди, які є найслабшою ланкою (наприклад, атака Stuxnet через USB-накопичувач).

Перевагою є те, що експерти, що мають глибоке розуміння системи, цілеспрямовано шукають вектори атак, здатні спричинити НСЕ, але з захисним мисленням.

3.2.3. Кількісна оцінка ймовірнісних відносин

Кількісна складова моделювання Байєсової мережі переконань використовує таблиці умовних імовірностей (CPT) для точного визначення ймовірнісних взаємозв'язків між вузлами. Наприклад, розглянемо атаку, що чинить вплив на систему, критичну для безпеки, A_1, і цей вплив представлений у відповідній CPT (як показано на рис. 3.3).

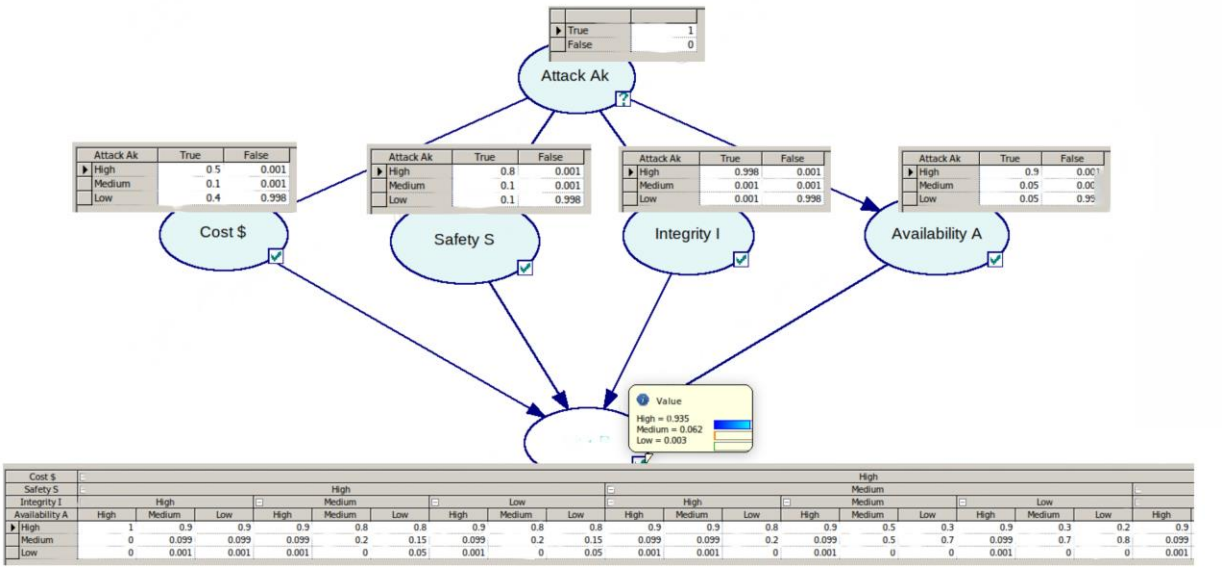


Рис. 3.3. Таблиця умовних імовірностей атаки A_1 на систему A

У даній роботі CPT-значення, що відображають вплив на безпеку, цілісність та доступність (SIA), є вищими. Це обґрунтовано тим, що порушення SIA у критичній інфраструктурі може призвести до катастрофічних наслідків, включно з людськими жертвами.

Приклади катастрофічних дій. Атака A_1 на водоочисну станцію, що спричиняє отруєння питної води шляхом несанкціонованого підвищення концентрації хімічних речовин (наприклад, перевищення прийнятного рівня). Це може призвести до знищення цілої громади.

Атака, що деактивує пристрій життєзабезпечення, спричиняючи смерть пацієнта. Моделюючий інструмент GeNIe використовується для розрахунку загального впливу за умови здійснення атаки. Наприклад, результат обчислення демонструє, що певна атака спричиняє загальний вплив на систему A у 93,5% (тобто, ризик R=93,5%).

Робустність вихідних ймовірностей мережі BBN визначається за допомогою аналізу чутливості (SA). Моделер GeNIe обчислює чутливість усіх можливих параметрів CPT відносно цільового вузла або набору цільових вузлів.

Алгоритм SA, реалізований у GeNIe, генерує набір похідних. Ці похідні ґрунтуються на наборі доказів у мережі та є критично важливими для оцінки точності числових параметрів мережі при обчисленні апостеріорних ймовірностей цільових вузлів. Чутливість кожного вузла в мережі BBN кількісно виражається як дійсне значення похідної та як набір коефіцієнтів, відповідно до рівняння. Набір коефіцієнтів встановлює залежність між цільовим апостеріорним вузлом (P) та конкретним параметром CPT (u).

$$P = \frac{(au + b)}{(cu + d)^2}$$

де P — апостеріорна ціль, a,b,c,d — коефіцієнти, обчислені SMILE (Structural Modeling, Inference, and Learning Engine), а u — значення конкретного параметра CPT.

Похідна D розраховується за формулою:

$$D = \frac{(ad - bc)}{(cu + d)}$$

За допомогою рівняння та похідної D визначається ступінь, на який зміниться апостеріорна ціль при зміні значень u. Ступінь цієї зміни визначається граничними значеннями $u_1 = b/d$ та $u_2 = (a+b) / (c+d)$.

Моделер GeNIe візуально розрізняє чутливі вузли в мережі, використовуючи колірне кодування : сірий колір позначає нечутливі вузли, рожевий/світло-червоний — малозначні, а червоний — високочутливі вузли (як показано на рисунку 3.4).

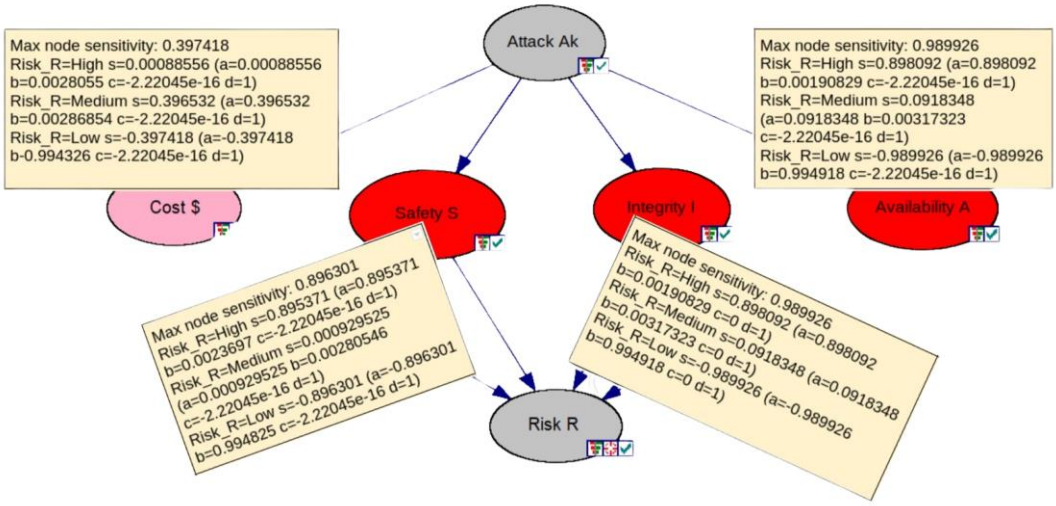


Рис. 3.4. Аналіз чутливості атаки A_1 на систему A

Аналіз чутливості (SA) - це методика, яка використовується для перевірки робастності та надійності моделі BBN. SA вимірює, наскільки сильно зміна одного вхідного параметра (у даному випадку, ймовірності в CPT, пов'язаної з атакою A_1) впливає на кінцевий результат (апостеріорну ймовірність), наприклад, на загальний ризик R.

Результати аналізу чутливості для критичних факторів SIAC показують: вузли безпеки (Safety), цілісності (Integrity) та доступності (Availability) демонструють чутливість 90%, 99% та 99% відповідно.

Вузол вартість (Cost) має чутливість 40%.

Ця кількісна інформація є критично важливою для процесу прийняття рішень, оскільки дозволяє спрямовувати обмежені ресурси на пом'якшення

тих атак або дій, які впливають на високочутливі вузли, максимізуючи ефективність захисних заходів.

Таблиця 3.1.

Стратегічні висновки для інженерії кібербезпеки

Фактор	Чутливість	Інтерпретація	Стратегічні наслідки
Цілісність (I)	99%	Найвища критичність. Навіть найменша неточність в оцінці ймовірності успіху атаки на цілісність різко змінює кінцеву оцінку HCE-ризику.	Необхідні найжорсткіші заходи захисту: валідація даних датчиків, криптографічні хеші для команд керування, системи виявлення маніпуляцій.
Доступність (A)	99%	Надзвичайно висока критичність. Атаки, спрямовані на відмову системи (DOS/ DDoS), можуть бути менш імовірними, але їхній вплив на кінцевий ризик є майже прямим і максимальним.	Інвестиції у надлишковість (резервні канали зв'язку, дублюючі контролери), механізми захисту від перевантаження мережі та географічно розподілені сервери.
Безпека (S)	90%	Висока чутливість, що підтверджує прямий зв'язок між порушенням умов безпеки (наприклад, вихід тиску за межі) та HCE.	Впровадження захисних механізмів, які гарантують, що кіберзагроза не може перевести фізичні процеси у недопустимий стан.
Вартість (C)	40%	Найменш чутливий параметр. Хоча фінансові збитки є значними, вони не є основним драйвером ймовірності катастрофічного HCE.	Витрати на виробництво чи ремонт мають нижчий пріоритет для негайного захисту, ніж запобігання фізичній шкоді та людським втратам.

Таким чином, SA перетворює якісну гіпотезу ("атака на цілісність небезпечна") на кількісно обґрунтоване рішення ("інвестуйте X у захист цілісності, оскільки помилка в оцінці цього ризику матиме найбільшу похибку у плануванні").

Висновки до розділу

Отже, в цьому розділі представлено імплементацію IT-моделей оцінки ризиків кібербезпеки та методи їх інтеграції у процеси проєктування і моніторингу технологічних процесів. Запропоновано інтегровану методологію пріоритизації подій у керуванні промисловими системами, що базується на принципах кіберінформованого інжинірингу та Байєсових мереж переконань. Такий підхід забезпечує можливість побудови ймовірнісних моделей взаємозв'язку між технічними параметрами, поведінковими характеристиками системи та рівнем ризику кіберінцидентів.

Розроблена методологія дозволяє:

- динамічно оцінювати ризики в реальному часі;
- здійснювати кількісну оцінку ймовірнісних відносин між подіями;
- оптимізувати пріоритети реагування на інциденти;
- підвищити рівень адаптивності системи керування до непередбачуваних загроз.

Таким чином, реалізація запропонованих моделей і методів дає змогу створити єдину структуру управління безпекою промислових систем, що інтегрує процеси оцінки ризиків, контролю подій та прийняття рішень на основі даних.

ВИСНОВКИ

В магістерській роботі розглянуто здійснено дослідження теоретичних, методологічних та прикладних аспектів розроблення ІТ-моделей проєктування промислових систем керування та моніторингу технологічних процесів, спрямованих на забезпечення їхньої функціональної безпеки, надійності та кіберзахищеності.

У процесі дослідження проаналізовано сучасний стан предметної області, визначено архітектуру, структуру та принципи функціонування промислових систем керування (ПСК), охарактеризовано основні компоненти — програмовані логічні контролери (PLC), SCADA-системи, датчики, виконавчі механізми та канали комунікації. Показано, що в умовах цифровізації та переходу до концепції «Індустрія 4.0» традиційні методи проєктування ПСК потребують модернізації з урахуванням зростання кіберзагроз та взаємозалежності інформаційних і технологічних рівнів.

Обґрунтовано доцільність використання кіберінформованого підходу до проєктування, який інтегрує принципи системної інженерії, аналізу ризиків і кібербезпеки. Розроблено комплексну методологію забезпечення стійкості промислових систем, що охоплює процеси оцінки ризиків, управління загрозами, визначення критичних точок взаємодії між підсистемами безпеки та захисту, а також формування процедур стійкого проєктування.

Проведено дослідження конфліктів між вимогами безпеки та захищеності промислових систем. Запропоновано підхід до їх аналізу та усунення, який поєднує методи системного процес-аналізу, інтегрованого управління ризиками та навчання на основі конфліктів. Це дозволяє узгоджувати технічні, організаційні та інформаційні вимоги під час розроблення систем керування, мінімізуючи ризики порушення їх цілісності та функціональної надійності.

Розроблено ІТ-моделі оцінки ризиків кібербезпеки, засновані на Байєсових мережах переконань, що забезпечують можливість кількісного аналізу взаємозв’язків між подіями, вразливостями та ймовірностями інцидентів. Такий підхід уможливлює побудову інтелектуальної системи підтримки прийняття рішень для моніторингу та керування технологічними процесами в реальному часі.

Експериментальна імплементація розробленої методології в контексті конкретного технологічного процесу підтвердила її ефективність: забезпечено зниження рівня невизначеності в оцінці ризиків, підвищення точності прогнозування можливих інцидентів та покращення узгодженості між вимогами функціональної безпеки й кіберзахисту.

У результаті виконання роботи:

- сформовано науково обґрунтовану методологію проєктування промислових систем керування з урахуванням факторів кібербезпеки;

- запропоновано ІТ-моделі для аналізу, моніторингу та оптимізації технологічних процесів;

- доведено ефективність підходу кіберінформованого інжинірингу для забезпечення стійкості промислових систем до кіберзагроз.

Отже, магістерська робота має як теоретичне, так і практичне значення, оскільки результати дослідження можуть бути використані при розробленні, впровадженні та експлуатації промислових систем нового покоління, що поєднують високий рівень автоматизації, безпеки та кіберстійкості.

ПЕРЕЛІК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. McLaughlin, S., Konstantinou, C., Wang, X., Davi, L., Sadeghi, A.-R., Maniatakos, M., & Karri, R. (2020). The cybersecurity landscape in Industrial Control Systems (ICS).
2. Bhamare, D., Zolanvari, M., Erbad, A., Jain, R., Khan, K., & Meskin, N. (2020). Cybersecurity for Industrial Control Systems: A survey. Computers & Security.
3. Elmarkez, A., Mesli-Kesraoui, S., Berruet, P., & Oquendo, F. (2025). Security by Design for Industrial Control Systems from a Cyber-Physical System Perspective: A Systematic Mapping Study. Machines, 13(7), 538.
4. Aslam, M. M., … (2025). Artificial intelligence for secure and sustainable industrial automation. International Journal of Intelligent Systems.
5. Chockalingam, S. (2021). Bayesian network model to distinguish between intentional attacks and technical failures in floodgates. Cybersecurity and Critical Infrastructure Protection Journal.
6. (2010). A Bayesian Network Methodology for Infrastructure Seismic Risk Assessment and Decision Support. University of California eScholarship.
7. Straub, D., & Der Kiureghian, A. (2012). Bayesian Network Enhanced with Structural Reliability Methods: Methodology. ArXiv preprint.
8. Straub, D., & Der Kiureghian, A. (2012). Bayesian Network Enhanced with Structural Reliability Methods: Application. ArXiv preprint.
9. (2023). Real-time risk assessment and decision support using Bayesian network. IChemE Conference Poster.
10. (2022). Risk analysis methodology using STPA-based Bayesian network. Reliability Engineering & System Safety.
11. (2025). A dynamic Bayesian network approach to characterize multi-hazard risk. Reliability Engineering & System Safety.
12.

13.(2024). Dynamic risk assessment in cybersecurity: A systematic literature review. Future Internet, 15(10), 324.
14. Sakovych, B., Zharikova, M., & Sherstjuk, V. (2022). The Probabilistic Graphical Model for Multi-Hazard Risk Evaluation of Critical Infrastructure Impairment. CEUR Workshop Proceedings.
15. Krotofil, M., Cardenas, A. A., Manning, B., & Sandberg, H. (2014). CPS: Cyber-physical systems attack analysis using graph-based models. In Proceedings of the IEEE Conference on Control Applications (pp. 447–454). IEEE. https://doi.org/10.1109/CCA.2014.6981367
16. Chockalingam, S., et al. (2021). Bayesian network model to distinguish between intentional attacks and technical failures in floodgates. Cybersecurity and Critical Infrastructure Protection. SpringerOpen. https://doi.org/10.1186/s42400-021-00086-6
17. Bhamare, D., Zolanvari, M., Erbad, A., Jain, R., Khan, K., & Meskin, N. (2020). Cybersecurity for Industrial Control Systems: A Survey. Computers & Security. https://arxiv.org/abs/2002.04124
18. Lee, C., & Der Kiureghian, A. (2010). A Bayesian network methodology for infrastructure seismic risk assessment and decision support. (Doctoral thesis). University of California. https://escholarship.org/uc/item/4vn733bh
19. Reniers, G., & et al. (2022). Risk analysis methodology using STPA-based Bayesian network. Reliability Engineering & System Safety, https://doi.org/10.1016/j.ress.2022.02.005
20. Sakovych, B., Zharikova, M., & Sherstjuk, V. (2022). The probabilistic graphical model for multi-hazard risk evaluation of critical infrastructure impairment. CEUR Workshop Proceedings, 3422, … ([ceur-ws.org])
21. Conti, M., Donadel, D., & Turrin, F. (2021). A survey on industrial control system testbeds and datasets for security research. arXiv preprint. https://arxiv.org/abs/2102.05631
22. Umer, M. A., Junejo, K. N., Jilani, M. T., & Mathur, A. P. (2022). Machine learning for intrusion detection in industrial control systems: Applications,

challenges, and recommendations. arXiv preprint. https://arxiv.org/abs/2202.11917

23. Christopher, J. (2024, October 16). The 2024 state of ICS/OT cybersecurity: Our past and our future. SANS Institute Blog. https://www.sans.org/blog/the-2024-state-of-ics-ot-cybersecurity-our-past-and-our-future

24. “Dynamic risk assessment in cybersecurity: A systematic literature review.” (2024). Future Internet, 15(10), 324. https://doi.org/10.3390/fi15100324

25. Huitsing, P., Chandia, R., Papa, M., & Shenoi, S. (2008). Attack taxonomies for industrial control systems. International Journal of Critical Infrastructure Protection, 1(1), 37–44. https://doi.org/10.1016/j.ijcip.2008.08.003

26. Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., & Stoddart, K. (2016). A review of cyber security risk assessment methods for SCADA systems. Computers & Security, 56, 1–27. https://doi.org/10.1016/j.cose.2015.09.009

27. Galloway, B., & Hancke, G. P. (2013). Introduction to industrial control networks. IEEE Communications Surveys & Tutorials, 15(2), 860–880. https://doi.org/10.1109/SURV.2012.072312.00028

28. Knowles, W., Prince, D., Hutchison, D., Disso, J. F., & Jones, K. (2015). A survey of cyber security management in industrial control systems. International Journal of Critical Infrastructure Protection, 9, 52–80. https://doi.org/10.1016/j.ijcip.2015.02.002

29. Humayed, A., Lin, J., Li, F., & Luo, B. (2017). Cyber-physical systems security—A survey. IEEE Internet of Things Journal, 4(6), 1802–1831. https://doi.org/10.1109/JIOT.2017.2703172

30. Zhu, B., Joseph, A., & Sastry, S. (2011). A taxonomy of cyber attacks on SCADA systems. In Proceedings of the 2011 IEEE International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing (pp. 380–388). IEEE. https://doi.org/10.1109/iThings/CPSCom.2011.34

31. Kharchenko, V., Illiashenko, O., & Morozov, V. (2019). Cybersecurity of critical infrastructures: State, problems, and trends. Information and Security: An International Journal, 44(1), 47–58. https://doi.org/10.11610/isij.4404
32. Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., & Hahn, A. (2015). Guide to industrial control systems (ICS) security (NIST Special Publication 800-82 Rev. 2). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-82r2
33. Leitão, P., Colombo, A. W., & Karnouskos, S. (2016). Industrial automation based on cyber-physical systems technologies: Prototype implementations and challenges. Computers in Industry, 81, 11–25. https://doi.org/10.1016/j.compind.2015.08.004
34. Ekelhart, A., Fenz, S., & Neubauer, T. (2020). AURUM: A framework for risk management of IT infrastructures. International Journal of Information Management, 50, 1–10. https://doi.org/10.1016/j.ijinfomgt.2019.05.009