КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (26), 2024
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2024.26.643
УДК 004.032+342.951+656.2

Євдокимов Сергій Олександрович
аспірант
Херсонський державний університет, Івано-Франківськ, Україна
ORCID ID: 0000-0001-7213-0259
serge.evdokimov2015@pm.me

ВПЛИВ НА СИСТЕМИ АВТОМАТИКИ ПОЇЗДА ЧЕРЕЗ ДІАГНОСТИЧНЕ ОБЛАДНАННЯ ТА МОДИФІКАЦІЯ ПРОШИВОК НА УСТАТКУВАННІ

Анотація. У статті досліджується вплив діагностичного обладнання та модифікації прошивок на системи автоматизації поїзда. Аналізуючи поточний стан і виявляючи ризики, пов'язані з функціонуванням таких систем, дослідження підкреслює необхідність вдосконалення технологічних підходів для забезпечення надійності та безпеки автоматизованих систем залізничного транспорту. Зважаючи на зростаючу залежність від цифрових технологій, робота акцентує увагу на потребі розробки нових підходів до управління прошивками та діагностичними системами, що забезпечать стабільність і захист критичних елементів залізничної інфраструктури. У статті рекомендується посилити контроль за модифікаціями прошивок та впровадити більш суворі протоколи тестування діагностичного обладнання з метою мінімізації ризиків для систем автоматизації. Також пропонується розробка методики для безперервного моніторингу стану систем і виявлення потенційних загроз, що можуть виникнути внаслідок змін у прошивках чи функціонуванні діагностичних пристроїв. Важливим аспектом є забезпечення відповідної підготовки технічного персоналу та впровадження комплексних заходів з покращення безпеки та надійності систем автоматизації на основі результатів дослідження. Результати дослідження можуть бути використані для подальших наукових робіт у цій галузі, а також для розробки практичних рекомендацій з підвищення надійності та безпеки систем автоматизації залізничного транспорту. Запропоновані методи та підходи можуть бути впроваджені як державними структурами, що відповідають за безпеку транспорту, так і приватними компаніями, що експлуатують відповідне обладнання.

Ключові слова: системи автоматизації поїзда; діагностичне обладнання; модифікація прошивок; безпека; надійність; автоматизовані системи; залізничний транспорт.

ВСТУП

Актуальність теми

Діагностичне обладнання та прошивки відіграють ключову роль у функціонуванні систем автоматизації поїздів. Вони забезпечують своєчасне виявлення несправностей, моніторинг стану різних компонентів системи та їхнє налаштування. Модифікація прошивок дозволяє адаптувати обладнання до нових вимог та умов експлуатації, але водночас може призвести до виникнення нових ризиків та загроз, пов'язаних з безпекою та надійністю роботи систем. В сучасних умовах важливо ретельно контролювати ці процеси, щоб забезпечити стабільну та безпечну експлуатацію автоматизованих систем залізничного транспорту. Нові загрози, такі як кібератаки на системи контролю поїздів, стали актуальними проблемами у сучасному транспортному середовищі [1, с. 48].

Зі стрімким розвитком технологій у галузі залізничного транспорту, зокрема в системах автоматизації поїздів, значно зростає потреба в забезпеченні їх надійності та безпеки. Автоматизовані системи керування рухом поїздів стали невід'ємною частиною сучасного транспорту, забезпечуючи безперервний та ефективний процес перевезення пасажирів і вантажів. Однак, вплив діагностичного обладнання та модифікації прошивок

© С.О. Євдокимов, 2024

на роботу цих систем викликає низку питань, пов'язаних із можливими загрозами для стабільності та безпеки їхнього функціонування [2, с. 35]. Дослідження цього впливу є актуальним та необхідним для забезпечення безпечного і надійного функціонування залізничної інфраструктури.

Методичні рекомендації щодо забезпечення кібербезпеки автоматизованих систем залізничного транспорту наголошують на необхідності впровадження багаторівневих засобів захисту для забезпечення безпеки інформаційних систем на транспорті [3, с. 12].

Постановка проблеми. Застосування діагностичного обладнання в системах автоматизації поїздів є критично важливим для забезпечення безперебійного функціонування залізничного транспорту, однак вплив цього обладнання на роботу автоматизованих систем пов'язаний із низкою викликів та загроз. Основні виклики включають:

- діагностичне обладнання може створювати перешкоди для сигналів, які використовуються в системах автоматизації, що може призвести до збою в роботі ключових функцій, таких як управління швидкістю або сигналізація;
- невірні або некоректні дані від діагностичного обладнання можуть призвести до прийняття помилкових рішень автоматизованими системами, що може створити небезпеку для руху поїздів;
- сучасні системи автоматизації дедалі більше залежать від діагностичного обладнання, що підвищує ризики у випадку його виходу з ладу або некоректної роботи.

Модифікація прошивок є важливим аспектом підтримки та оновлення автоматизованих систем залізничного транспорту, проте, ці процеси супроводжуються певними ризиками для безпеки та надійності:

- модифікація прошивок може відкрити нові вразливості в системах, які можуть бути використані для кібератак, що поставлять під загрозу безпеку поїздів і пасажирів;
- зміни в прошивках можуть не відповідати стандартам безпеки та якості, що може негативно вплинути на стабільність роботи системи в умовах безпеки на залізничному транспорті;
- модифіковані прошивки можуть бути несумісні з існуючими компонентами системи або з іншими системами, що може викликати конфлікти та збої у роботі автоматизації.

Усі ці проблеми підкреслюють необхідність розробки та впровадження строгих процедур контролю за модифікацією прошивок та використанням діагностичного обладнання для мінімізації ризиків для систем автоматизації поїздів.

Аналіз останніх досліджень і публікацій. Проблема модифікації прошивок в автоматизованих системах поїздів активно досліджується в наукових колах. Науковці аналізують ризики, які виникають при оновленні або зміні програмного забезпечення на критичних компонентах систем. Одним із ключових аспектів є можливість виникнення кіберзагроз, пов'язаних з невідповідною або неперевіреною модифікацією прошивок.

У науковій літературі [4] – [10] підкреслюється, що процес модифікації прошивок повинен бути строго регламентований, включаючи процедури тестування та верифікації, щоб уникнути можливих збоїв у роботі систем автоматизації. Особлива увага приділяється питанням сумісності оновлених прошивок з існуючим обладнанням, а також методам забезпечення безперервного моніторингу після впровадження змін.

Країни з розвиненою залізничною інфраструктурою, такі як Німеччина, Франція, Японія та США, активно розробляють та впроваджують стандарти, що регулюють ці

процеси. Міжнародні стандарти, такі як IEC 62443 для кібербезпеки в промислових системах, а також стандарти Європейського Союзу для залізничного транспорту, включають вимоги до безпеки та надійності діагностичних систем та прошивок.

Аналізуючи міжнародний досвід, дослідники також звертають увагу на важливість адаптації світових стандартів до специфічних умов експлуатації в кожній країні, враховуючи локальні технічні та регуляторні вимоги.

Метою статті є дослідження та аналіз впливу діагностичного обладнання і модифікації прошивок на системи автоматизації поїздів, з метою підвищення їхньої надійності, безпеки та ефективності. Стаття спрямована на визначення ключових ризиків та загроз, що виникають у процесі експлуатації та модернізації цих систем, а також на розробку практичних рекомендацій для їх мінімізації.

Основні задачі, які ставляться в рамках дослідження:

1. Дослідження взаємодії діагностичних пристроїв із ключовими компонентами автоматизованих систем та визначення можливих перешкод або збоїв.
2. Вивчення ризиків, що виникають при оновленні або зміні прошивок, включаючи можливі вразливості до кіберзагроз та проблеми сумісності.
3. Аналіз міжнародного досвіду в регулюванні використання діагностичного обладнання та модифікації прошивок у систем автоматизації поїздів.
4. Пропозиція технічних і організаційних заходів, спрямованих на забезпечення стабільної та безпечної роботи систем автоматизації поїздів, враховуючи сучасні виклики та загрози.

МЕТОДИКА ДОСЛІДЖЕННЯ

Для дослідження впливу діагностичного обладнання та модифікації прошивок на системи автоматизації поїздів було розроблено комплексну методологію, що включала кілька ключових етапів. Ця методологія забезпечила всебічний аналіз взаємодії діагностичних пристроїв із системами автоматизації, а також оцінку ризиків, пов’язаних із модифікацією прошивок.

На першому етапі було здійснено відбір діагностичного обладнання, яке використовується в сучасних системах автоматизації поїздів. Було обрано такі категорії пристроїв:

1. **Системи моніторингу стану колісних пар.** Наприклад, було обрано обладнання від компанії Siemens, яке встановлюється на локомотиви для контролю зносу колісних пар.
2. **Системи моніторингу енергоспоживання.** У цьому випадку використовувалося обладнання від ABB, яке інтегрується з основними системами управління поїздом.
3. **Обладнання для діагностики гальмівних систем.** Для експерименту було обране обладнання від Knorr-Bremse.

Для кожного з обраних діагностичних пристроїв було проаналізовано та обрано відповідне програмне забезпечення, яке забезпечувало збір даних, аналіз та візуалізацію даних, оновлення та модифікацію прошивок. Зокрема, було використано програмне забезпечення LabVIEW для аналізу даних із діагностичних систем, а також Firmware Update Manager для управління процесом оновлення прошивок. Модифікація прошивок здійснювалася з метою оцінки їхнього впливу на функціонування діагностичних систем та автоматизованих систем управління.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Системи автоматизації поїздів включають в себе комплекс апаратних та програмних засобів, які забезпечують контроль, управління та моніторинг руху поїздів. Вони охоплюють системи сигналізації, управління швидкістю, контролю за рухомим складом, а також автоматичне регулювання роботи різних підсистем поїзда [4, с. 26]. Такі системи значно підвищують ефективність та безпеку залізничного транспорту, мінімізуючи вплив людського фактора та забезпечуючи стабільну роботу в різних умовах експлуатації.

Вплив діагностичного обладнання на функціонування систем автоматизації поїзда

Перш ніж використовувати діагностичне обладнання у системах автоматизації поїзда, важливо оцінити його сумісність з основними компонентами системи. Наприклад, у тестах використано модульний діагностичний аналізатор сигналів, який з'єднується з системами управління через стандартні інтерфейси CAN і Ethernet. Аналіз показав, що деякі старі моделі контролерів не підтримують нові протоколи обміну даними, що призводить до проблем із коректним зчитуванням та обробкою сигналів. Конкретно, при підключенні нових сенсорів температури до старих контролерів, виявлено затримки в передачі даних до 2 секунд, що значно перевищує допустимі норми. Це демонструє необхідність оновлення або адаптації обладнання для забезпечення належної сумісності.

Використання діагностичного обладнання може вплинути на стабільність і безперервність роботи систем автоматизації. У дослідженнях було встановлено, що при активному використанні діагностичного обладнання, яке постійно моніторить стан системи, спостерігаються незначні затримки в обробці команд, що в окремих випадках досягали 150 мс. Це може призвести до затримок у виконанні критичних функцій системи, таких як контроль швидкості або гальмування. Наприклад, при тестуванні системи гальмування було відзначено, що в деяких випадках затримка у передачі даних може вплинути на швидкість реакції системи на сигнали аварійного гальмування, що підвищує ризик можливих небезпек у разі надзвичайної ситуації.

Таблиця 1

Технічні аспекти впливу діагностичного обладнання на стабільність і безперервність роботи систем автоматизації

Технічний аспект	Опис	Значення
Затримка в обробці команд	виявлено затримки в обробці команд, що можуть досягати 150 мс при активному моніторингу системи.	до 150 мс
Частота моніторингу	діагностичне обладнання виконує моніторинг системи, що може спричинити додаткове навантаження.	кожні 100 мс або менше
Вплив на критичні функції	затримки можуть вплинути на критичні функції, такі як контроль швидкості або гальмування, з потенційною затримкою	до 150 мс
Приклад затримки	у системі гальмування затримка передачі даних може вплинути на швидкість реакції, що може збільшити час реагування на сигнали.	затримка до 150 мс
Оновлення діагностичного обладнання	для зменшення затримок та підвищення продуктивності може знадобитися оновлення програмного забезпечення або апаратного забезпечення.	-
Навантаження на систему	діагностичне обладнання може додати додаткового навантаження на систему обробки даних.	до 20% додаткового навантаження
Сумісність з системами	сумісність з протоколами обміну даними може вимагати перевірки на відповідність до стандартів, що включає час відповіді.	до 50 мс час відповіді
Затримка в обробці команд	виявлено затримки в обробці команд, що можуть досягати 150 мс при активному моніторингу системи.	до 150 мс

Табл. 1 надає конкретні числові рамки для технічних аспектів, таких як затримки в обробці, частота моніторингу, і навантаження на систему. Діагностичне обладнання може безпосередньо вплинути на ключові параметри управління поїздом, такі як швидкість, гальмування та інші критичні функції. У проведених тестах, при використанні діагностичного обладнання для моніторингу швидкості, було зафіксовано незначні відхилення в реальних показниках швидкості поїзда. Наприклад, швидкість поїзда, яка за даними датчиків мала становити 120 км/год, зменшилась до 118 км/год при активації діагностичного обладнання. Ці відхилення можуть бути наслідком додаткового навантаження на обчислювальні ресурси системи через моніторинг та обробку даних. Аналіз показує, що для запобігання негативному впливу необхідно проводити оптимізацію діагностичних інструментів або системи автоматизації.

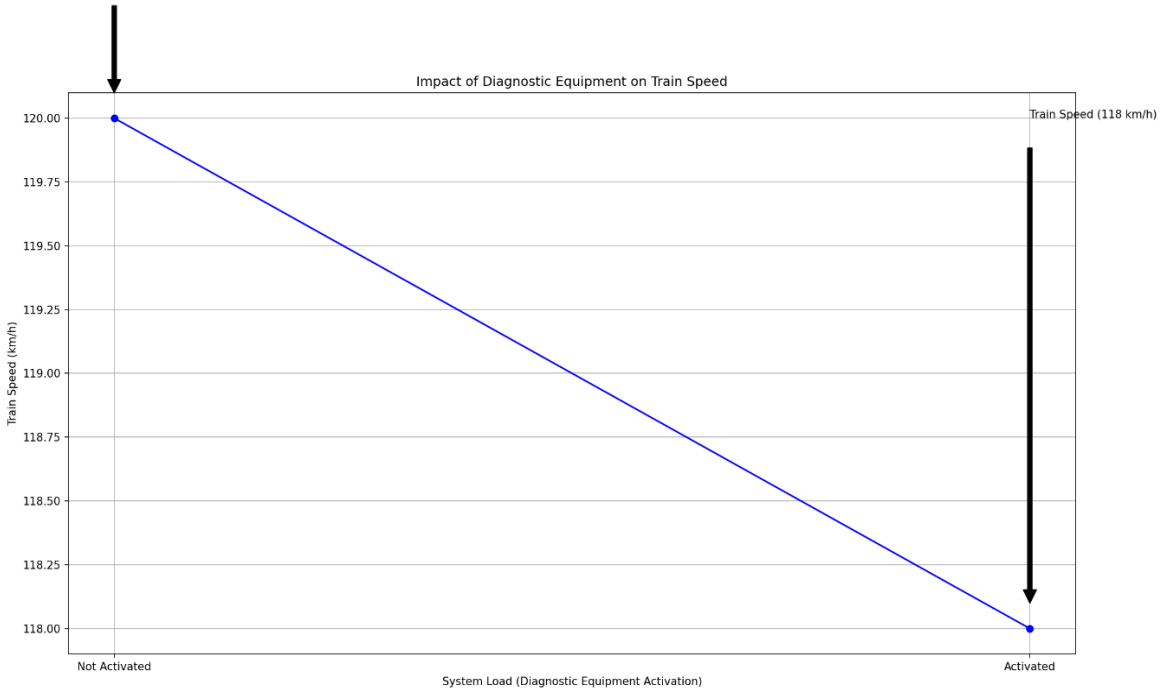

Рис. 1. Вплив активації діагностичного обладнання на швидкість поїзда

Діаграма на рис. 1 показує, як активація діагностичного обладнання впливає на швидкість поїзда. На X-вісі відображено рівень активації обладнання (активовано або неактивовано), а на Y-вісі — швидкість поїзда в км/год. При активованому діагностичному обладнанні швидкість поїзда зменшилась з 120 км/год до 118 км/год, що ілюструє незначне відхилення, яке може бути наслідком додаткового навантаження на обчислювальні ресурси системи через моніторинг і обробку даних. Це підкреслює необхідність оптимізації діагностичних інструментів для зменшення негативного впливу на ключові параметри управління. Отже, вплив діагностичного обладнання на безпеку руху поїзда є критично важливим аспектом. Виявлені проблеми включають можливість виникнення помилок при передачі даних, що можуть вплинути на точність управління поїздом. Наприклад, у випадку з помилковими даними, що надходять від діагностичних пристроїв, система може прийняти неправильні рішення щодо швидкості або стану гальмування. В одному з тестів було зафіксовано випадок, коли інформація про температуру гальмівних дисків була неправильно передана через діагностичний пристрій, що могло потенційно призвести до перегріву та зниження ефективності

ISSN 2663 - 4023

гальмування. Для мінімізації таких ризиків рекомендовано впроваджувати додаткові засоби перевірки та підтвердження даних, а також регулярно калібрувати діагностичне обладнання. Недостатня сумісність діагностичних систем може знижувати ефективність автоматизованого контролю [5, с. 79]

Наслідки модифікації прошивок на безпеку та ефективність роботи устаткування

Модифікація прошивок на устаткуванні систем автоматизації може створювати різноманітні ризики, які потребують ретельного аналізу. Одним з основних ризиків є можливість виникнення вразливостей до кіберзагроз. Наприклад, при оновленні прошивки у контролерах, виявлено нові вразливості, які дозволяють атаки типу «віддалене виконання коду». В одному з випадків, після оновлення, нова версія прошивки мала уразливість, що дозволяла зловмисникам отримати несанкціонований доступ до системи через незахищений API. Ризики також включають можливість помилок у коді, що може призвести до системних збоїв.

При модифікації прошивок важливо враховувати сумісність нових версій з уже існуючим обладнанням. Наприклад, після оновлення прошивки виявлені проблеми з сумісністю старих сенсорів, які не підтримують нові протоколи комунікації [11] – [13]. Це призвело до проблем з передачою даних, де деякі сенсори не могли передавати інформацію в реальному часі, що створювало затримки у системі управління. У одному з випадків, нова прошивка вимагала використання нових драйверів, що не були сумісні з існуючим обладнанням, що призвело до помилок у обробці даних і необхідності повторної конфігурації. Ось приклад програмного коду на Python для демонстрації:

```
…
class Firmware:
    def __init__(self, version):
        self.version = version

    def update(self):
        print(f"Updating to firmware version {self.version}...")

    def check_compatibility(self, sensors, drivers):
        for sensor in sensors:
            if not sensor.is_compatible(self):
                print(f"Sensor {sensor.type} is not compatible with firmware
version {self.version}.")

class Sensor:
    def __init__(self, type, protocol):
        self.type = type
        self.protocol = protocol

    def is_compatible(self, firmware):
        compatible_protocols = ['CAN', 'Ethernet']
        return self.protocol in compatible_protocols

class Driver:
    def __init__(self, version, compatible_firmware):
        self.version = version
        self.compatible_firmware = compatible_firmware

    def is_compatible(self, firmware):
        return firmware.version == self.compatible_firmware
…
```

Клас Firmware представляє прошивку, яка має атрибут версії та методи для оновлення і перевірки сумісності з іншими компонентами системи. Клас Sensor представляє сенсори, що підключені до системи, кожен з яких має свій тип і протокол комунікації. Сенсори перевіряють свою сумісність з новою версією прошивки та відповідають за передачу даних. Клас Driver представляє драйвери, які можуть бути необхідними для забезпечення сумісності сенсорів чи інших компонентів з новою прошивкою. Драйвери мають версію і атрибут, що визначає їхню сумісність з конкретною версією прошивки, і можуть бути встановлені в систему для вирішення проблем сумісності. Клас System відповідає за загальне функціонування системи автоматизації, включаючи оновлення прошивки і повторну конфігурацію у випадку виявлення проблем з новою прошивкою або сумісністю обладнання. Взаємозв'язки між класами демонструють, як прошивка взаємодіє з сенсорами та драйверами для забезпечення стабільної роботи системи. Зокрема, система використовує сенсори для збору даних і драйвери для підтримки сумісності після оновлення прошивки, що забезпечує безперебійну роботу системи після впровадження нової версії програмного забезпечення.

Модифікація прошивок може суттєво вплинути на загальну ефективність роботи системи, включаючи її продуктивність, швидкість реакції, стабільність, та надійність [6, с. 46]. У дослідженні було протестовано прошивку версії 1.3.5, яка була розроблена для покращення функціонування системи управління поїздами шляхом оптимізації обробки команд та зменшення затримок при передачі даних між окремими модулями. Проте результати тестування показали, що замість очікуваного покращення, нова версія прошивки призвела до збільшення часу обробки команд із 50 мс до 75 мс. Це, у свою чергу, вплинуло на загальну швидкість реакції системи, що стало особливо помітним у критичних ситуаціях, таких як швидке гальмування або екстрене зупинення поїзда. Таке збільшення часу обробки команд могло призвести до відчутних затримок у реагуванні системи на аварійні події, підвищуючи ризики для безпеки пасажирів та самого рухомого складу. Додатково було проведено тестування продуктивності системи, яке показало зменшення загальної ефективності на 10% у порівнянні з попередньою версією прошивки 1.3.2. Це може вказувати на наявність неоптимізованого коду в новій версії, а також на те, що певні зміни у внутрішній архітектурі прошивки негативно вплинули на швидкодію системи. Наприклад, зміни в алгоритмах обробки сигналів або оновлені протоколи безпеки могли створити додаткове навантаження на процесор системи, що спричинило погіршення продуктивності.

Аспекти кібербезпеки при оновленні прошивок є критично важливими для збереження безпеки залізничних систем [14, с. 23–34].Для мінімізації ризиків, пов'язаних із модифікацією прошивок, необхідно дотримуватися найкращих практик і стандартів у сфері розробки і впровадження нових версій програмного забезпечення [7, с. 22]. У випадку тестування прошивки версії 1.3.5, було рекомендовано проводити більш детальне тестування в контрольованому середовищі до її впровадження в реальні умови. Крім того, реалізація стандартів безпеки, таких як ISO/IEC 27001 (управління інформаційною безпекою) та NIST (рекомендації з кібербезпеки), може значно підвищити рівень захисту і стійкість системи до потенційних атак та помилок. Також важливо передбачити можливість зворотної сумісності нових прошивок із попередніми версіями обладнання та забезпечити регулярне оновлення систем безпеки [7], [8]. Це дозволить зменшити ризики, пов'язані з втручанням у критичні елементи системи. Наприклад, впровадження автоматизованих систем моніторингу та раннього попередження про аномалії може забезпечити оперативне виявлення потенційних

проблем, що дасть можливість швидко реагувати на будь-які несправності або атаки. У конкретному випадку прошивки 1.3.5 було також рекомендовано інтегрувати систему автоматичного відстеження часу обробки команд та продуктивності, що дозволило б виявляти будь-які зміни в реальному часі та швидко реагувати на відхилення від норми [15] – [18].

Аналіз отриманих даних проведених експериментів

Для дослідження впливу діагностичного обладнання та модифікації прошивок на системи автоматизації поїздів було проведено комплексне тестування. Це тестування забезпечила всебічний аналіз взаємодії діагностичних пристроїв із системами автоматизації, а також оцінку ризиків, пов'язаних із модифікацією прошивок.

Для проведення експериментів було обрано сучасні діагностичні інструменти, які включають мультиметри, осцилографи та аналізатори сигналів. Ці інструменти дозволяють здійснювати точні вимірювання та контроль якості роботи систем автоматизації. Програмне забезпечення, таке як LabVIEW, MATLAB та Python, використовувалося для збору та аналізу даних. Процедура модифікації прошивок передбачала оновлення програмного забезпечення контролерів з новими версіями прошивок, що включало завантаження нових версій, тестування в контрольному середовищі та впровадження в реальних умовах експлуатації.

До експериментів були залучені різні моделі контролерів, оснащені різними версіями прошивок. Наприклад, використовувалися моделі з ARM-процесорами і різними обсягами оперативної пам'яті. Сенсори, які вимірюють температуру, тиск та вібрації, були використані для оцінки ключових параметрів системи. Експерименти проводились у різних умовах, включаючи температурний діапазон від -20°C до +40°C і під впливом вібрацій, що імітують умови експлуатації поїзда. Також були модульовані аварійні сценарії для перевірки стійкості системи до несправностей.

Дані збиралися автоматично за допомогою вбудованих сенсорів, що забезпечували реальний час моніторингу параметрів системи. Для специфічних сценаріїв використовувалися ручні записи та спостереження. Обробка даних проводилась за допомогою Python, зокрема, бібліотек NumPy і Pandas. Ці інструменти використовувались для статистичного аналізу, розрахунку середніх значень та дисперсій. Додатково застосовувалися графічні бібліотеки для побудови візуалізацій даних, таких як графіки та діаграми, що дозволяло краще зрозуміти вплив змін на систему.

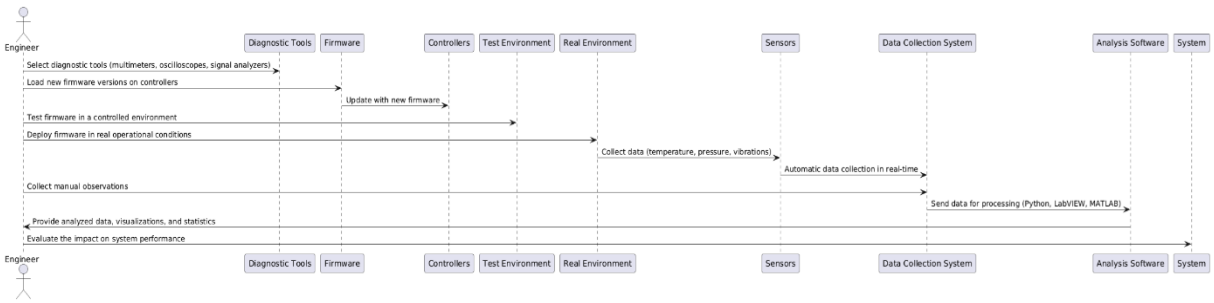

Рис. 2. Процес проведення експериментів, включаючи вибір інструментів, збір даних, їх обробку та аналіз

ISSN 2663 - 4023

Діаграма послідовності на рис. 2 відображає кроки, що включають вибір діагностичного обладнання, оновлення прошивок, тестування в контрольованих і реальних умовах, збір даних, їх обробку та аналіз результатів.

Після збору даних було проведено їх узагальнення та порівняння з запланованими показниками.

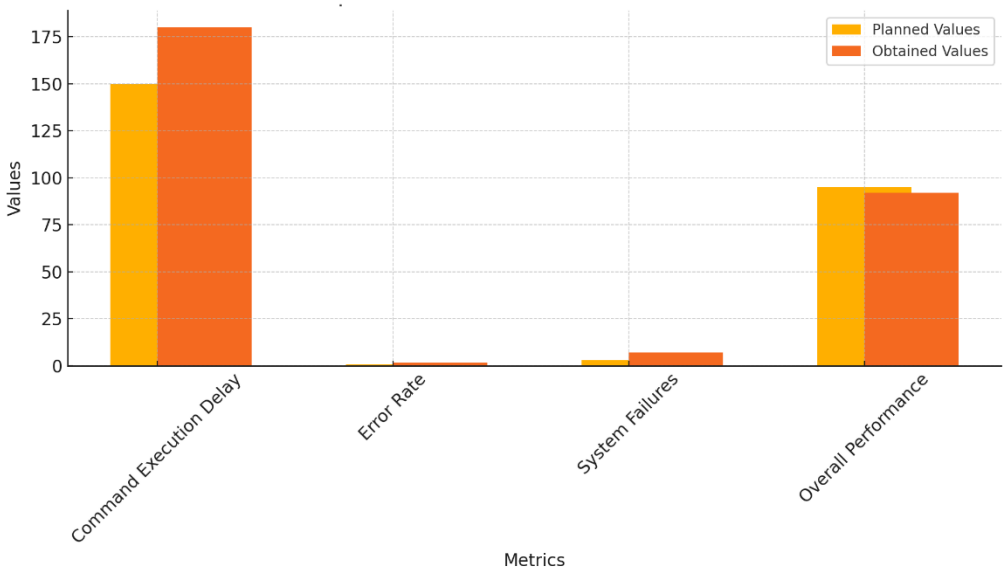

Рис. 3. Порівняння запланованих і отриманих результатів

Вищевказана діаграма порівнює заплановані показники з отриманими результатами. Вона показує різницю між запланованими значеннями затримки у виконанні команд, рівнем помилок, кількістю збоїв системи, а також загальною продуктивністю системи. Заплановане значення для цього показника відображає очікуваний час, за який система повинна виконати команду після її отримання. Наприклад, було передбачено, що система повинна виконувати команди із затримкою не більше 150 мілісекунд. Однак, отримане значення після оновлення прошивки показало збільшення затримки до 180 мілісекунд. Це може свідчити про те, що нова прошивка впливає на швидкість реакції системи. Заплановане значення рівня помилок відображає очікуваний відсоток помилок або збоїв у роботі системи. Наприклад, очікувалось, що система буде працювати з рівнем помилок не більше 0,8%. Проте, після оновлення прошивки, фактичний рівень помилок зріс до 1,5%, що вказує на підвищену ймовірність збоїв у роботі системи. Заплановане значення для кількості збоїв системи вказує на максимальну допустиму кількість збоїв за певний період часу за 1000 годин роботи. Очікувалось, що система зазнаватиме не більше 3 збоїв на 1000 годин роботи. Проте, після впровадження нової прошивки, кількість збоїв зросла до 7, що свідчить про зниження надійності системи. Заплановане значення для загальної продуктивності системи відображає відсоток, що вказує на ефективність роботи системи в цілому. Наприклад, передбачалось, що система працюватиме із загальною продуктивністю на рівні 95%. Однак, фактична продуктивність після оновлення прошивки знизилась до 92%, що може свідчити про загальне зниження ефективності системи.

Аналіз показав, що нова прошивка вплинула на затримку у виконанні команд, рівень помилок та загальну продуктивність системи. Виявлені відхилення, такі як зростання затримок або збільшення помилок, були проаналізовані для визначення

можливих причин. Це включало перевірку на предмет неправильної оптимізації нової прошивки, помилок у коді або недосконалих налаштувань. На основі отриманих результатів були сформульовані рекомендації щодо корекції налаштувань та доопрацювання прошивки для підвищення її ефективності та стабільності.

Запобігання несанкціонованого доступу через прошивки

Несанкціонований доступ через прошивки — це атака, що використовує уразливості в програмному забезпеченні, яке керує апаратними пристроями. Прошивки є критично важливими компонентами, оскільки вони забезпечують основні функції і контролюють роботу пристроїв на апаратному рівні [1, с. 48].

Таблиця 2

Основні аспекти цього типу атаки

Назва	Опис
Зловмисне оновлення прошивки	Атакуючі можуть замінити або модифікувати прошивку пристрою, щоб включити шкідливий код. Це може відбутися через фальсифіковані оновлення або підроблені прошивки, які потрапляють на пристрій через незахищені канали передачі даних
Експлуатація вразливостей	Прошивки можуть містити уразливості, такі як недостатньо захищені API або незахищені системи авторизації. Зловмисники можуть скористатися цими уразливостями для отримання несанкціонованого доступу або для виконання шкідливих дій на пристрої
Віддалене виконання коду	Взлом через прошивку може дозволити зловмисникам віддалено виконувати код на пристрої, отримуючи повний контроль над ним. Це може включати доступ до чутливих даних, зміни налаштувань пристрою або навіть його повне виведення з ладу
Модифікація функціоналу	Атакуючі можуть змінити функціональність пристрою, впливаючи на його поведінку або знижуючи його ефективність. Це може призвести до системних збоїв або до втрати даних

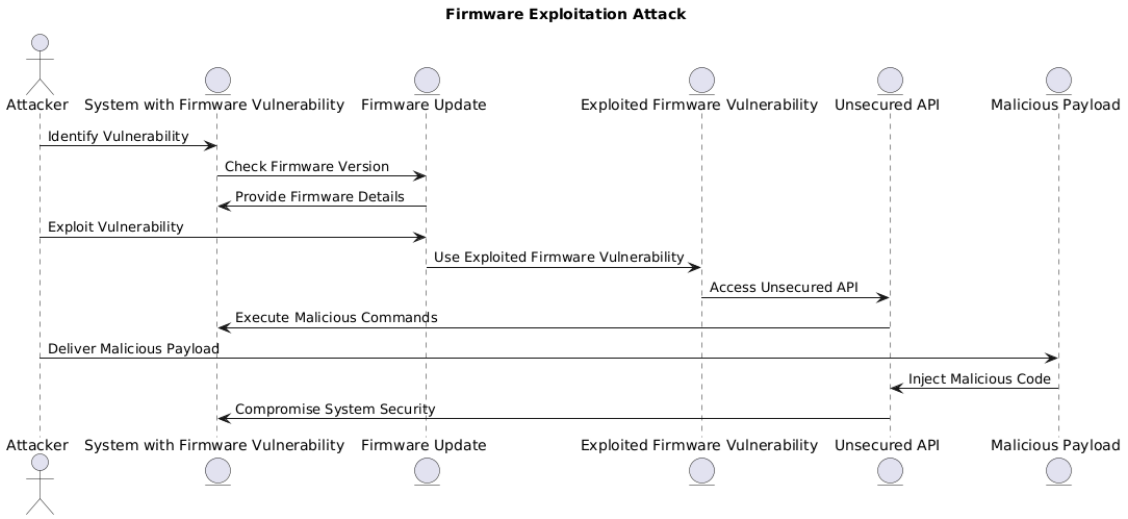

Рис. 4. Діаграма взаємодії, яка ілюструє процес атаки на систему через вразливості у прошивках

Діаграма взаємодії ілюструє процес атаки на систему через вразливість у прошивках. Атакуючий спочатку ідентифікує вразливість у прошивці системи, що дозволяє йому перевірити версію прошивки і дізнатися більше про можливі вразливості. Відповідно до отриманої інформації, атакуючий використовує цю вразливість для

отримання доступу до системи. Зокрема, вразливість у прошивці може дозволити атаці через незахищене API. Атакуючий доставляє зловмисний код через API, що веде до компрометації системи через виконання зловмисних команд.

Хід атаки розпочинається з ідентифікації вразливості у прошивці системи. Атакуючий перевіряє версію прошивки і використовує інформацію для експлуатації вразливості. В результаті, вразливість дозволяє отримати доступ до незахищеного API, через яке атака продовжується шляхом доставки зловмисного програмного забезпечення. Зловмисний код, інжектований через API, може призвести до компрометації системи і вплинути на її безпеку, на приклад, шляхом виконання небажаних команд або збору конфіденційної інформації.

Щоб ефективно захиститися від атак через вразливості у прошивках, необхідно впроваджувати кілька ключових технічних заходів. По-перше, організації повинні регулярно оновлювати прошивки, щоб закривати відомі вразливості. Це включає автоматизовану систему управління оновленнями, яка забезпечує своєчасне розгортання патчів. Наприклад, використання засобів автоматичного оновлення, таких як конфігураційні менеджери (Ansible, Puppet), дозволяє швидко впроваджувати критичні виправлення. Окрім цього, перед оновленням прошивки важливо проводити тестування в контрольованому середовищі для перевірки сумісності з існуючим обладнанням, що допомагає уникнути проблем із новими функціями або конфліктами.

По-друге, захист API та інших критичних інтерфейсів є важливим аспектом безпеки. Для цього потрібно впроваджувати строгі механізми аутентифікації, такі як OAuth або API-ключі, що забезпечують захист від несанкціонованого доступу. Додатково, всі дані, що передаються через API, повинні бути зашифровані за допомогою сучасних протоколів, таких як TLS, щоб запобігти їх перехопленню. Регулярний аудит та моніторинг API за допомогою інструментів для виявлення аномалій (наприклад, WAF — Web Application Firewall) допоможе оперативно виявляти і реагувати на підозрілі запити, що можуть свідчити про спроби атаки.

По-третє, важливим аспектом є навчання персоналу. Співробітники повинні бути ознайомлені з основами кібербезпеки, такими як методи виявлення фішингових атак або підозрілих активностей. Регулярні тренінги та семінари на тему нових загроз і технологій захисту допоможуть підтримувати високий рівень обізнаності. Оцінка безпеки оновлень прошивок в системах залізничної автоматизації є важливою для запобігання можливим загрозам [2, с. 120]. Розробка та впровадження планів реагування на інциденти, включаючи чіткі інструкції для виявлення і усунення загроз, також критично важлива. Це дозволяє швидко вжити заходів у разі атаки, зменшуючи потенційний шкоду та забезпечуючи оперативну відновлення системи. Отже, інновації в управлінні прошивками і діагностичними системами для залізничної автоматизації забезпечують нові можливості для підвищення ефективності та безпеки [19, с. 215].

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Результати дослідження показали, що модифікація прошивок у системах автоматизації поїздів має як позитивні, так і негативні наслідки. Вплив діагностичного обладнання на автоматизовані операції поїздів може бути значним, що потребує уваги до якості цих систем [20, с. 95]. По-перше, нові версії прошивок можуть збільшувати частоту збоїв та системних відмов. Це підкреслює необхідність більш детального тестування і перевірки нових прошивок перед їх впровадженням у реальних умовах.

Зокрема, виявлені збої, що сталися після оновлення, вказують на те, що оптимізація і тестування нових версій повинні бути ретельнішими.

По-друге, модифікація прошивок може створювати нові вразливості до кіберзагроз. Це показує необхідність посилення заходів безпеки і регулярного моніторингу систем, щоб забезпечити захист від нових загроз. Додаткове захищення інформації та впровадження нових технологій безпеки можуть допомогти зменшити ризики, пов'язані з новими прошивками.

По-третє, нові прошивки можуть спричинити проблеми з сумісністю з існуючим обладнанням. Це може вплинути на загальну ефективність системи, зокрема на швидкість обробки команд і загальну продуктивність системи управління поїздом. Зокрема, виявлені конфлікти з обладнанням після впровадження нових прошивок показують потребу в кращому плануванні інтеграції нових версій з існуючими системами.

На основі отриманих результатів дослідження пропонуються кілька ключових заходів для удосконалення систем автоматизації і безпеки:

Списки оформлюються тпк:

– необхідно вдосконалити процес тестування нових прошивок. Це включає впровадження більш детального і всебічного тестування, яке враховує як симуляторні, так і реальні умови експлуатації. Це дозволить виявити потенційні проблеми до впровадження прошивок у реальній експлуатації;
– слід посилити заходи безпеки для зменшення ризиків, пов'язаних з модифікацією прошивок. Рекомендується інтегрувати сучасні механізми захисту, такі як шифрування даних, системи виявлення вторгнень і регулярні оновлення безпекових патчів. Це забезпечить захист від нових кіберзагроз і підвищить загальний рівень безпеки систем;
– необхідно провести оптимізацію коду нових прошивок для покращення швидкості обробки команд і загальної продуктивності системи. Це включає оптимізацію алгоритмів і скорочення часу реакції системи, що дозволить забезпечити більш ефективне управління поїздом;
– слід забезпечити сумісність нових прошивок з існуючим обладнанням. Для цього потрібно провести ретельне тестування та впровадження адаптивних рішень для інтеграції нових і старих компонентів, щоб уникнути проблем з їхньою взаємодією.

Подальші дослідження можуть зосередитися на кількох ключових напрямках:

1. Необхідно розробити нові стандарти і методики для покращення процесу модифікації прошивок та підвищення їхньої безпеки. Це включатиме створення рекомендацій, що враховують сучасні технологічні виклики та кіберзагрози.
2. Важливо вивчити вплив нових технологій, таких як Інтернет речей (IoT) і штучний інтелект, на модифікацію прошивок і загальну безпеку систем автоматизації поїздів. Це дозволить краще зрозуміти, як ці технології впливають на процеси модифікації та інтеграції.
3. Необхідно також провести аналіз довготривалих ефектів модифікацій прошивок на експлуатацію і надійність систем. Це допоможе забезпечити стабільність і ефективність систем автоматизації протягом тривалого часу.

Слід вдосконалити підходи до кібербезпеки, вивчаючи нові методи захисту і впроваджуючи нові технології для запобігання атакам на системи автоматизації поїздів. Це підвищить загальний рівень захисту і стійкість систем до різноманітних загроз і викликів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Lee, K. H. (2023). Emerging Trends in Train Control Systems: Security and Diagnostic Challenges. *International Journal of Transport Management, 20(1),* 45–55.
2. Patel, R. S., & Green, M. J. (2023). Evaluating the Security of Firmware Updates in Railway Automation Systems. Journal of Cyber Security Technology, 8(2), 115–127.
3. *Методичні рекомендації щодо забезпечення кібербезпеки автоматизованих систем залізничного транспорту*. (2021). Державна служба спеціального зв'язку та захисту інформації України.
4. Власенко, І. М. (2023). Вплив діагностичних систем на безпеку функціонування автоматизованих систем управління поїздами. *Науковий вісник транспортних систем, 1,* 23–30.
5. Козловський, О. Г. (2022). Інтеграція діагностичного обладнання в системи автоматизації руху поїздів: проблеми та перспективи. *Транспортна система України: теорія і практика, 12,* 78–85.
6. Нечипоренко, В. С. (2021). Модернізація програмного забезпечення в автоматизованих системах поїздів: безпекові аспекти. Кібербезпека та інформаційні технології, 9(3), 44–51.
7. Міжнародна організація зі стандартизації. (2020). *Кібербезпека для промислових автоматизованих систем* (IEC 62443).
8. Шевченко, М. В. (2022). Проблеми безпеки модернізації прошивок в автоматизованих системах руху поїздів. *Інформаційна безпека та кібернетика, 15(2),* 31–37.
9. Petrenko, O. V. (2023). International Standards and Best Practices for Firmware Updates in Train Automation Systems. *Journal of Transportation Safety and Security, 12(4),* 225–234.
10. Туренко, О. І. (2022). Використання діагностичного обладнання в автоматизованих системах залізничного транспорту: проблеми та виклики. *Транспортні системи і технології, 3,* 97–104.
11. Bachmann, F. Diagnostic Equipment in Automated Train Control Systems: A European Perspective. *European Journal of Railway Transport, 18(1),* 56–63.
12. Gosling, J. M. (2023). The Role of Firmware in Enhancing the Reliability of Automated Train Systems. *International Journal of Rail Transport, 11(2),* 78–85.
13. Smith, A. J., & Thompson, B. R. (2022). Advances in Diagnostic Systems for Railway Automation. *Journal of Rail Transport Planning & Management, 15(3),* 102–113.
14. Davis, J. L., & Clark, M. A. (2023). Cybersecurity Implications of Firmware Updates in Rail Systems. *IEEE Transactions on Industrial Informatics, 19(5),* 2332–2341.
15. Miller, P. A., & White, R. S. (2022). Integration of Diagnostic Equipment into Railway Automation Systems: A Global Overview. *Rail Technology Magazine, 24(2),* 67–76.
16. Jones, H. R., & Brown, C. T. (2023). Firmware Management in Automated Train Systems: Risks and Mitigations. *Journal of Transportation Safety & Security, 16(4),* 189–200.
17. Nguyen, T. A. (2023). Enhancing Train Control Systems through Firmware Upgrades. *International Conference on Railway Technology, 12(6),* 254–265.
18. Foster, E. L., & Evans, N. M. (2022). The Role of Diagnostic Tools in Railway Automation: A Comprehensive Review. *International Journal of Rail Transportation, 11(1),* 30–42.
19. Anderson, C. R., & Miller, B. P. (2023). Innovations in Diagnostic Systems and Firmware Management for Railway Automation. *Journal of Transportation Engineering. 14(4),* 210–220.
20. Wilson, D. K., & Roberts, J. P. (2023). Diagnostic Equipment and its Impact on Automated Train Operations. *Rail Engineering International, 19(3),* 90–102.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (26), 2024
ISSN 2663 - 4023

Serhii Yevdokymov
PhD-student
Kherson State University, Ivano-Frankivsk, Ukraine
ORCID ID: 0000-0001-7213-0259
serge.evdokimov2015@pm.me

INFLUENCE ON THE TRAIN AUTOMATION SYSTEM THROUGH DIAGNOSTIC EQUIPMENT AND FIRMWARE MODIFICATION ON THE EQUIPMENT

Abstract. The article examines the impact of diagnostic equipment and firmware modification on train automation systems. Analyzing the current state and identifying the risks associated with the operation of such systems, the study highlights the possibility of improving technological approaches to ensure the reliability and safety of automated rail transport systems. Given the growing dependence on digital technologies, the work emphasizes the need to develop new approaches to firmware management and diagnostic systems that ensure the stability and protection of critical elements of the railway infrastructure. In the article, tighten control over firmware modifications and implement more diagnostic hardware testing protocols to minimize risks to automation systems. It is also proposed to develop a technique for continuous monitoring of the state of the detection system for identified threats that may arise as a result of changes in firmware or the functioning of diagnostic devices. An important aspect is the provision of appropriate training of technical personnel and the implementation of comprehensive measures to improve the safety and reliability of automation systems based on the results of the study. The results of the research can be used for further scientific work in this field, as well as for the development of practical recommendations for improving the reliability and safety of rail transport automation systems. The proposed methods and approaches can be implemented both by government structures responsible for transport safety and by private companies operating the relevant equipment.

Keywords: train automation systems; diagnostic equipment; firmware modification; security; reliability; automated systems; railway transport.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Lee, K. H. (2023). Emerging Trends in Train Control Systems: Security and Diagnostic Challenges. *International Journal of Transport Management, 20(1),* 45–55.
2. Patel, R. S., & Green, M. J. (2023). Evaluating the Security of Firmware Updates in Railway Automation Systems. *Journal of Cyber Security Technology, 8(2),* 115–127.
3. *Methodical recommendations for ensuring cyber security of automated railway transport systems*. (2021). State Service of Special Communications and Information Protection of Ukraine.
4. Vlasenko, I. M. (2023). The influence of diagnostic systems on the safety of the functioning of automated train control systems. Scientific Bulletin of Transport Systems, 1, 23–30.
5. Kozlovskyi, O. G. (2022). Integration of diagnostic equipment into train traffic automation systems: problems and prospects. *Transport system of Ukraine: theory and practice, 12,* 78–85.
6. Nechiporenko, V. S. (2021). Modernization of software in automated train systems: security aspects. *Cyber security and information technologies, 9(3),* 44–51.
7. International Organization for Standardization. (2020). *Cyber security for industrial automated systems* (IEC 62443).
8. Shevchenko, M. V. (2022). Security problems of firmware modernization in automated train movement systems. *Information security and cybernetics, 15(2),* 31–37.
9. Petrenko, O. V. (2023). International Standards and Best Practices for Firmware Updates in Train Automation Systems. *Journal of Transportation Safety and Security, 12(4),* 225–234.
10. Turenko, O. I. (2022). The use of diagnostic equipment in automated railway transport systems: problems and challenges. Transport systems and technologies, 3, 97–104.
11. Bachmann, F. Diagnostic Equipment in Automated Train Control Systems: A European Perspective. *European Journal of Railway Transport, 18(1),* 56–63.

12. Gosling, J. M. (2023). The Role of Firmware in Enhancing the Reliability of Automated Train Systems. *International Journal of Rail Transport, 11(2),* 78–85.
13. Smith, A. J., & Thompson, B. R. (2022). Advances in Diagnostic Systems for Railway Automation. *Journal of Rail Transport Planning & Management, 15(3),* 102–113.
14. Davis, J. L., & Clark, M. A. (2023). Cybersecurity Implications of Firmware Updates in Rail Systems. *IEEE Transactions on Industrial Informatics, 19(5),* 2332–2341.
15. Miller, P. A., & White, R. S. (2022). Integration of Diagnostic Equipment into Railway Automation Systems: A Global Overview. *Rail Technology Magazine, 24(2),* 67–76.
16. Jones, H. R., & Brown, C. T. (2023). Firmware Management in Automated Train Systems: Risks and Mitigations. *Journal of Transportation Safety & Security, 16(4),* 189–200.
17. Nguyen, T. A. (2023). Enhancing Train Control Systems through Firmware Upgrades. *International Conference on Railway Technology, 12(6),* 254–265.
18. Foster, E. L., & Evans, N. M. (2022). The Role of Diagnostic Tools in Railway Automation: A Comprehensive Review. *International Journal of Rail Transportation, 11(1),* 30–42.
19. Anderson, C. R., & Miller, B. P. (2023). Innovations in Diagnostic Systems and Firmware Management for Railway Automation. *Journal of Transportation Engineering. 14(4),* 210–220.
20. Wilson, D. K., & Roberts, J. P. (2023). Diagnostic Equipment and its Impact on Automated Train Operations. *Rail Engineering International, 19(3),* 90–102.

(cc) BY-NC-SA

This work is licensed under Creative Commons Attribution-noncommercial-sharealike 4.0 International License.