Міністерство освіти і науки України
Прикарпатський національний університет імені Василя Стефаника
Кафедра комп'ютерної інженерії та електроніки
(повна назва кафедри)

Татунь Павло Ігорович
Pavlo Tatun

УДК 004:681.5

Спеціальність 123 «Комп'ютерна інженерія»
(шифр та назва спеціальності)

Кваліфікаційна робота
на здобуття освітньо-кваліфікаційного рівня бакалавр
(бакалавр, спеціаліст, магістр)

Оцінка та забезпечення безпеки вбудованих систем у сучасних автомобілях
Assessment and security of embedded systems in modern cars

Науковий керівник:
д.т.н, професор Когут І.Т.
Рецензент:

Івано-Франківськ
2024

Форм.	Зона	Поз.	*Позначення*	*Найменування*	К-ть	Прим.
			123. УДК 004:681.5	Алгоритм виконання атаки	1	
			123. УДК 004:681.5	Пояснювальна записка	85	

Змн.	*Арк.*	*№ докум.*	*Підп.*	*Дата*	123.КІ-41.21		
Разробив		Татунь П.І.			Специфікація	*Літ.*	*Арк.* 2 / *Аркушів*
Перевірив		Когут І.Т.					
Н. Конт.							
Затвердив							

АНОТАЦІЯ

Сучасний автомобіль розуміється як інтелектуальний мехатронний транспортний засіб, інтегрований із системою управління, що відповідає різним аспектам концепції «Індустрії 4.0». У ході дослідження було доведено, що в сучасному електромобілі можна керувати наступними модулями управління в транспортному засобі: внутрішнім освітленням, поворотником і функцією рульового управління.

Дана робота містить 85 ст., 2 табл., 45 рис., 1 дод., 19 джерел.

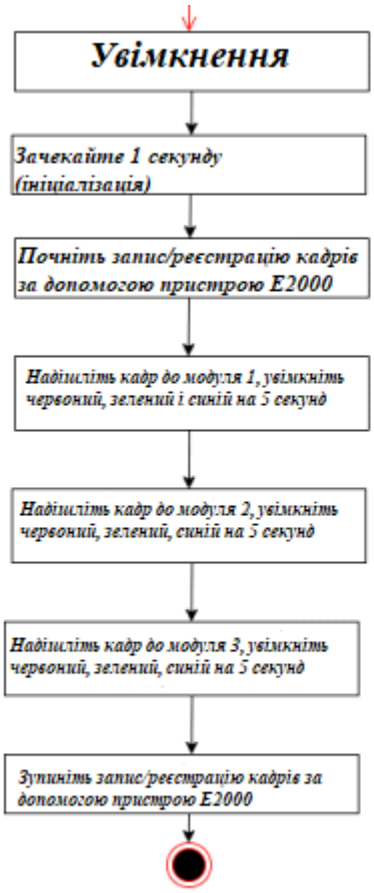
Змн.	*Арк.*	*№ докум.*	*Підпис*	*Дата*				
Розробив		Татунь П.І.			Анотація	*Літ.*	*Арк.*	*Аркушів*
Перевірив		Когут І.Т.					3	1
Н. Контр.		.						
Затвердив								

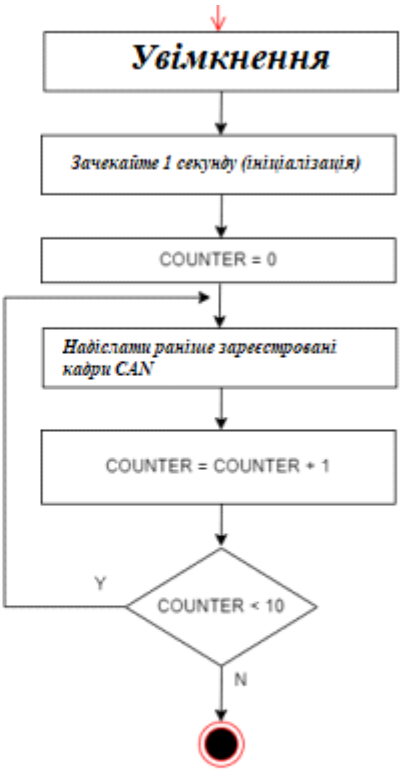
ABSTRACT

The modern car is developing as an intelligent mechatronic vehicle integrated with a control system that corresponds to various aspects of the concept of "Industry 4.0". In the course of the study, it was proven that in a modern electric car, the following control modules in the vehicle can be controlled: interior lighting, turn signal and steering function.

This work contains 85 articles, 2 table, 45 figures, 1 appendix, 19 sources.

Змн.	Арк.	№ докум.	Підпис	Дата			
Розробив		Татунь П.І.			ABSTRACT	Літ.	Арк. 4 / Аркушів 1
Перевірив		Когут І.Т.					
Н. Контр.		.					
Затвердив							





Змн.	Арк.	№ докум.	Підпис	Дата			
Розробив		Татунь П.І.			Алгоритм виконання атаки	Літ.	Арк. 5 / Аркушів 1
Перевірив		Когут І.Т.					
Н. Контр.		.					
Затвердив							

Державний вищий навчальний заклад
«Прикарпатський національний університет імені Василя Стефаника»
Фізико-технічний факультет
Кафедра комп’ютерної інженерії та електроніки

Пояснювальна записка
до кваліфікаційної роботи на тему

«Оцінка та забезпечення безпеки вбудованих систем у сучасних автомобілях»

					123.КІ-41.21			
Змн.	*Арк.*	*№ докум.*	*Підпис*	*Дата*				
Розробив		Татунь П.І.			. Пояснювальна записка	*Літ.*	*Арк.*	*Аркушів*
Перевірив		Когут І.Т.					6	85
Н. Контр.		.						
Затвердив								

ПЕРЕЛІК СКОРОЧЕНЬ

ABS - антиблокувальна система гальм

ADAS - передові системи допомоги водієві

AE - Auto Encoder

ШІ – штучний інтелект

BILSTM - двонаправлена довго-коротка пам'ять

CAN - мережа контролера

CAN FD - Гнучка передача даних контролера мережі

CRC - циклічна перевірка надмірності

DNN - глибока нейронна мережа

E2E - Наскрізний захист для передачі по CAN

ESC - електронний контроль стійкості

GPS - глобальна система позиціонування

GRU - Gated Recurrent Unit

GRU-AE – Gated Recurrent Unit – Autoencoder

IoT - Інтернет речей

LSTM - довготривала короткочасна пам'ять

ПК - персональний комп'ютер

ШІМ - широтно-імпульсна модуляція

TCS - система контролю тяги

TW – часове вікно

ЗМІСТ

ВСТУП

В епоху вдосконалення автоматизації, електромобільності та все більшого використання Інтернету, зокрема IoT (Інтернет речей), одним із найважливіших пріоритетів у галузі є виявлення загроз, які можуть виникнути у вбудованих системах. Особливо широко такі системи поширені в автомобільній промисловості. В автомобілях вони використовуються під час їх регулярної експлуатації в дорожньому русі, збираючи та обробляючи велику кількість даних.

В даний час атаки на такі системи спостерігаються все частіше. Щоб захистити вразливі дані та забезпечити безпеку пасажирів, необхідно розробити та впровадити підходи, спрямовані на усунення або принаймні мінімізацію ризиків атак.

Сучасні автомобілі є прикладами застосування технологій, пов’язаних з концепцією «Індустрії 4.0», де акцент робиться на інтеграції сучасних технологій, залучених до інтелектуального керування все більшою кількістю модулів, які спілкуються між собою.

Всі зусилля спрямовані на управління всіма можливими елементами і процесами в автомобілі за допомогою електронних модулів, з'єднаних між собою за допомогою роз'ємів, відомих як шини. Інтернет речей, будучи фундаментальним підходом у концепції Індустрії 4.0, останнім часом стрімко розвивається в автомобільному секторі. Це також відіграє важливу роль. Нові технології приносять багато зручностей і нових можливостей. На жаль, це також пов’язано з кількома потенційними ризиками, такими як:

- можливість крадіжки даних;
- дестабілізація роботи автомобіля (або будь-якого мехатронного пристрою);
- контроль над транспортним засобом (або будь-яким мехатронним пристроєм).

Враховуючи ці ризики, вбудовані системи керування автомобілем можуть прямо чи опосередковано вплинути на здоров’я та навіть життя людини. Наслідки втрати контролю можуть бути дуже серйозними.

Важливо підкреслити, що електромобілі, які живляться від акумуляторів, що накопичують велику кількість енергії, стають все більш популярними. Напруга становить сотні вольт. У випадку з цими автомобілями можна передбачити сценарій, коли через відсутність належного захисту модуля управління автомобіль може бути використаний не за призначенням. Тому необхідно пам'ятати про можливість атаки на вбудовані системи управління автомобіля і використовувати такі засоби захисту, які забезпечують безпеку користувачів. Існують різні види атак, і в найсерйознішій формі вони можуть знерухомити автомобіль. Слід підкреслити, що неможливо розробити повний і надійний захист від усіх форм атак, оскільки нові технології приносять також нові форми атак. Небезпечні ситуації, викликані атаками, здебільшого пов'язані з захопленням контролю над вибраними модулями, такими як гальмівна система та дестабілізація роботи автомобіля.

Мета даної роботи полягає в розробці підходів до мінімізації загроз у вбудованих автомобільних системах, які керують електронними модулями.

Завдання:

1. Розглянути існуючі системи безпеки вбудованих систем у сучасних автомобілях;
2. Проаналізувати функціональні характеристики вбудованих систем у сучасних автомобілях;
3. Описати методи обробки безпеки вбудованих систем;
4. Розглянути розробку та виявлення кібератак на рульовий механізм автомобіля.

РОЗДІЛ 1. ОГЛЯД ІСНУЮЧИХ СИСТЕМ ДЛЯ ОЦІНКИ ТА ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ВБУДОВАНИХ СИСТЕМ У СУЧАСНИХ АВТОМОБІЛЯХ

1.1. Сучасні автомобільні транспортні засоби

Ідея транспортного засобу з власним джерелом енергії, здатного брати на борт людей або вантажі, завжди була мрією людства. Початки машин з автономним приводом сягають часів першої промислової революції, коли був розроблений паровий двигун, який приводив у дію перші паровози. Це можна вважати проривом у наземному транспорті, оскільки величезні обсяги вантажів можна було перевозити на дуже великі відстані. Паралельно з громадським наземним транспортом розвивалася автомобільна промисловість. Особливо вона була спрямована на виробництво особового складу. Це дало велику самостійність у подорожах за менших витрат на підготовку дорожньої інфраструктури. Історія автомобільної промисловості починається з кінця 19 століття і винаходу першого двигуна внутрішнього згоряння, який встановлювався в автомобіль. Ці транспортні засоби являли собою складні механічні конструкції. Робота всіх основних модулів, відповідальних за водіння, гальмування та поворот, базувалася виключно на механічних системах [1].

Слід підкреслити, що на початку 20 століття електромобілі також були досить популярними, особливо в США. Вони мали обмежену дистанцію, але завдяки своїм перевагам, таким як безшумна робота двигуна, відсутність вихлопних газів і відсутність необхідності запускати механічним рукояткою, вони були особливо популярні серед жінок. На відміну від сучасних електромобілів, вони були транспортними засобами з повністю механічним керуванням.

На ранній стадії розвитку автомобільної промисловості керування транспортними засобами здійснювалося повністю механічно. Однак з його розвитком відбулися поступові зміни, пов’язані з інтеграцією електроніки та керування автомобілем, що призвело до збільшення частки мехатронних систем на користь механіки. Основні елементи мехатронної системи наведено на рис. 1.1.

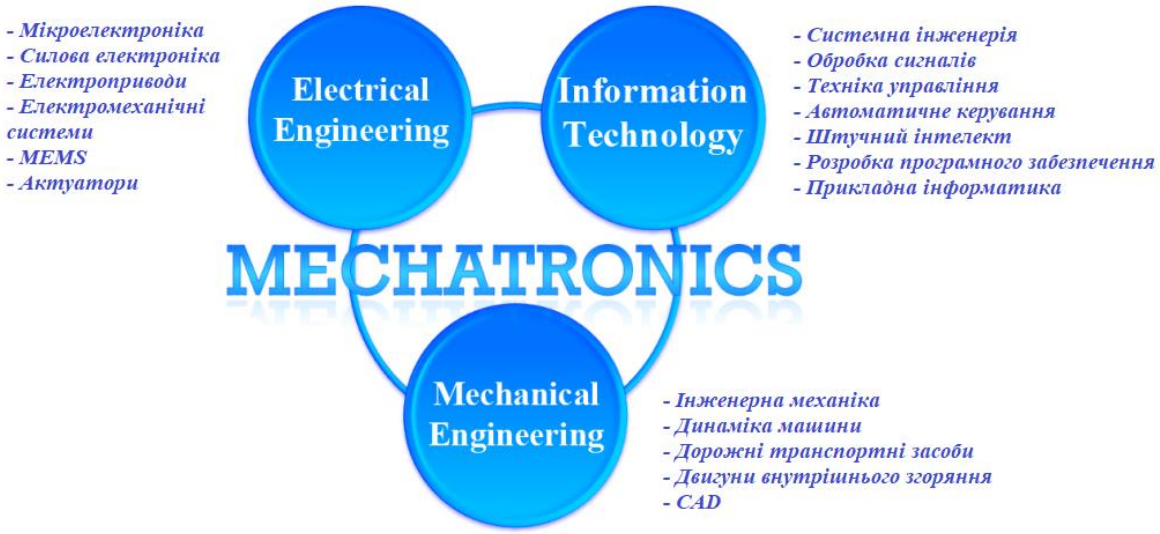


Рис.1.1. Інтеграція мехатронної системи

Ця поступова зміна, від механічних до мехатронних систем, була викликана дедалі вищими вимогами, пов’язаними з кращою продуктивністю, більшим комфортом і безпекою, а також оптимізацією споживання палива. Таким чином, типові механічні елементи поступово замінювалися елементами з електронним керуванням. Основні функціональні можливості та основні елементи сучасного автомобіля показані на рис. 1.2 та рис. 1.3.

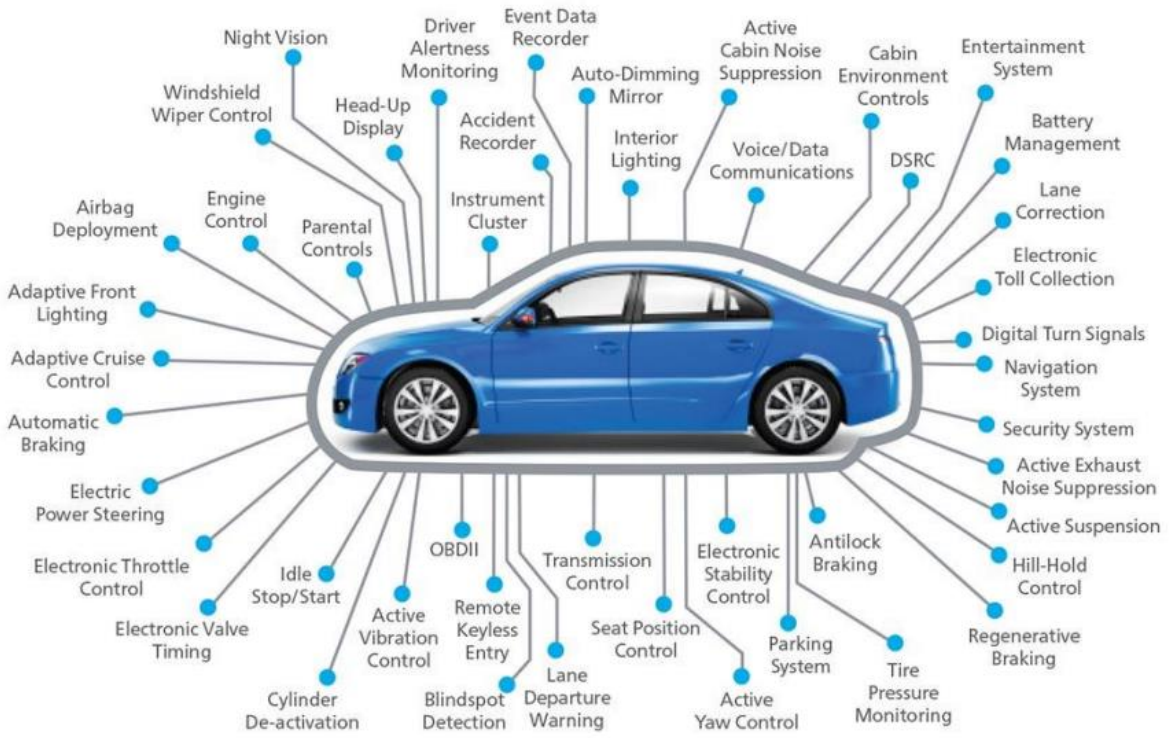


Рис.1.2. Основні функції сучасних автомобілів

Рис.1.3. Основні елементи сучасних автомобілів

Типовими прикладами спочатку механічних, а сьогодні мехатронних систем є системи повороту та гальмування (наприклад, ручне гальмо). Це два основні модулі керування автомобілем.

Типова механічна система ручного гальма, показана на рис. 1.4, відповідала за здатність блокувати задні колеса, щоб запобігти руху автомобіля в режимі паркування. У минулому це була система з'єднань зі сталевими тросами і регуляторами, відповідальними за рівномірний розподіл гальмівного зусилля на обидва задні колеса. Важливо, що продуктивність гальма також повинна бути оптимізована з точки зору функціональності, щоб не було потрібно багато зусилля для його використання. Його активація вимагає реакції водія. Важіль потрібно тягнути, і перш за все водій повинен про це пам'ятати. Механічне ручне гальмо управляється виключно водієм. Перевагою такого рішення є можливість ручного налаштування гальмівного зусилля і можливість його використання при спробі вийти з ковзання[2].

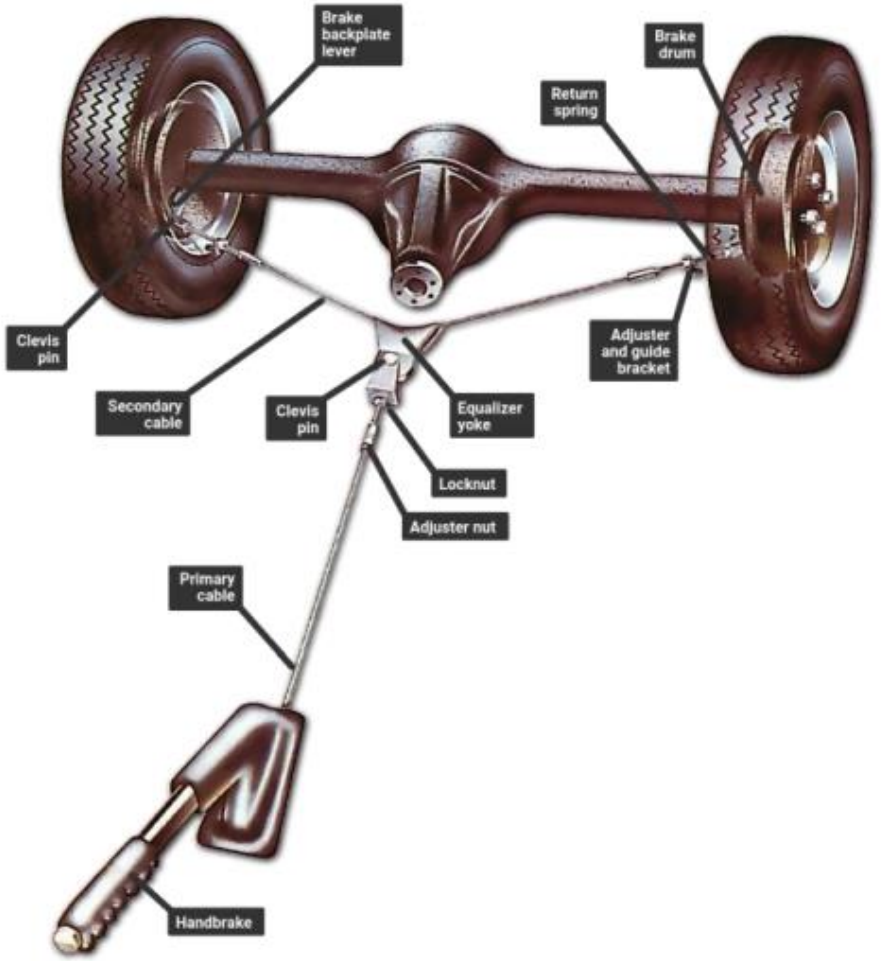


Рис.1.4. Механічна система ручного гальма в автомобілі

Наступником механічного ручного гальма є електронне стоянкове гальмо (іноді його називають електромеханічним стоянковим гальмом), яке є передовою мехатронною системою. Він керується сигналами, що надсилаються через шини передачі, тому немає необхідності використовувати дріт, що з'єднує передню та задню частини автомобіля. Рішення показано на рис. 1.5.

Рис.1.5. Електронне стоянкове гальмо

Зразкова виконавча система з приводом показана на рис. 1.6.

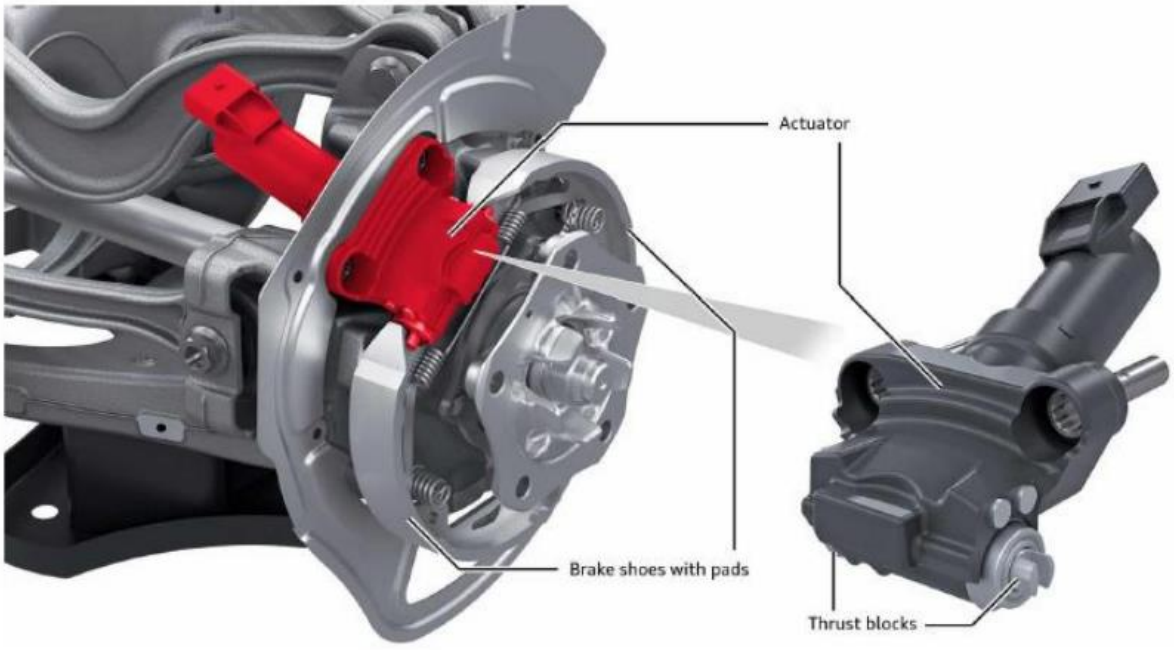


Рис.1.6. Гальмівна виконавча система з приводом

Можливість електронного керування стоянковим гальмом також розширює спектр його можливостей, включаючи можливість:

- блокування всіх коліс (а не однієї осі);
- автоматизація управління, активація/деактивація може здійснюватися в результаті дії водія, натиснувши кнопку на центральній консолі або системою керування транспортним засобом;
- екстрене гальмування за допомогою електромеханічного модуля стоянкового гальма.

Іншим прикладом трансформації механічних систем у мехатронні є система рульового управління. Ця система, поряд із системами водіння/прискорення та гальмування, відіграє одну з найважливіших функцій у роботі автомобіля. Реалізація цієї системи здебільшого пов'язана з двигуном автомобіля. На ранніх етапах розвитку автомобільної промисловості конструкція системи рульового керування, що відповідає за функцію повороту, також була виключно механічною. У разі механічного рішення рульове колесо з’єднане з рульовою колонкою, яка з’єднує рульове колесо з валом, який, у свою чергу, передає його рухи на рульовий механізм. Таке рішення забезпечує необхідну безпеку, оскільки після втрати потужності або гідравлічної підтримки все ще можна повертати колеса в автомобілі.

Послідовні мехатронні покоління систем рульового керування мають керувати за допомогою проводів. У цій концепції немає механічного зв'язку між кермом і трансмісією. Рульовий вал замінено сигнальними дротами, які з’єднують рульову колонку з рульовим механізмом, яким фізично керує електродвигун.

Концепції обох рішень керування гальмівною системою представлені на рис. 1.7. Версія А означає механічну, а версія В означає мехатронну систему керування.

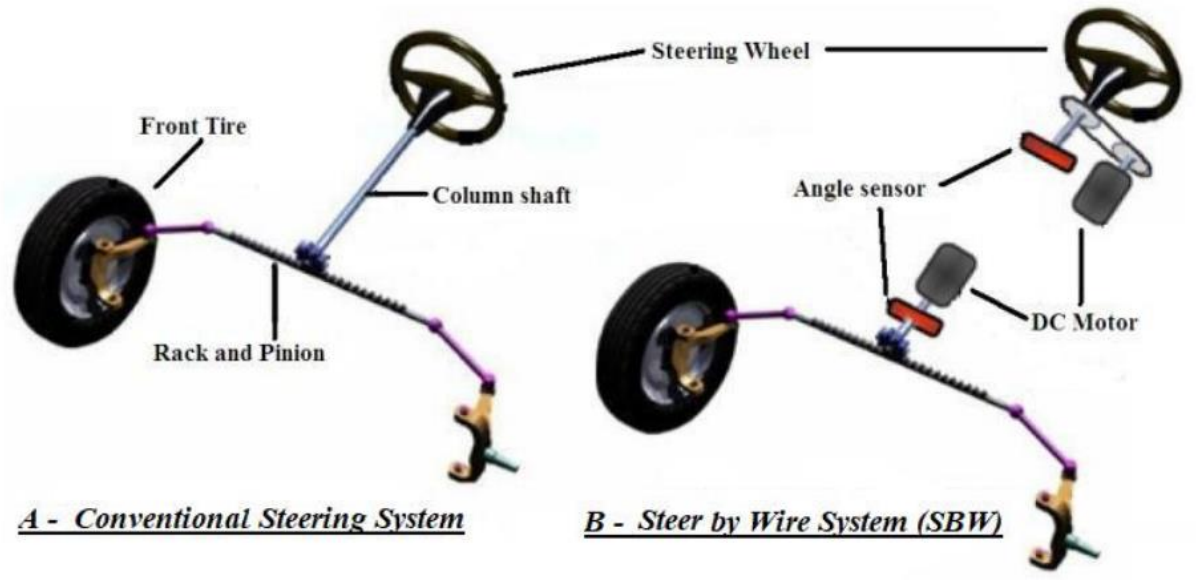


Рис.1.7. Концепції керування обома гальмівними системами

Слід підкреслити, що в сучасних автомобілях мехатронні системи складають основну частину систем керування. Без них, враховуючи запити користувачів, важко досягти реалізації необхідної функціональності автомобіля. До них належать [3]:

- Електронна система запалювання – система, що відповідає за подачу напруги на свічки запалювання двигуна внутрішнього згоряння;
- Антиблокувальна система гальм (ABS) – система, яка захищає автомобіль від блокування коліс під час різкого гальмування;
- Traction Control System (TCS) – система, що входить до групи Advanced Vehicle Control Systems, основним завданням якої є запобігання надмірного пробуксовування коліс автомобіля під час розгону, що проявляється їх пробуксовуванням. Система контролю тяги є частиною системи електронного контролю стійкості (ESC);
- Система круїз-контролю – система, яка дозволяє підтримувати задану швидкість без використання педалі газу;
- Система активної підвіски – система, що відповідає за утримання дороги, забезпечення стійкості та комфорту під час руху завдяки безперервному налаштуванню амортизації підвіски до дорожніх умов;

- Система подушок безпеки – система, що відповідає за захист голови та грудей водія та пасажирів у разі лобового зіткнення;
- Система замикання дверей – система, що відповідає за замикання та відмикання дверей. На додаток до стандартних операцій відкриття та закриття автомобіля за допомогою дистанційного ключа, він керує автоматичним блокуванням після перевищення певної швидкості або розблокуванням у разі аварії.

1.2. Сучасні напрямки розвитку систем мехатроніки автомобілів

Сучасний автомобіль містить значну кількість мехатронних модулів і елементів, які взаємодіють для оптимізації продуктивності або підвищення безпеки та комфорту водіння. Сьогодні мехатроніка відіграє ключову роль у процесі перетворення транспортних засобів на розумні та ефективні транспортні засоби, починаючи від керування двигуном, оптимізації автоматичних коробок передач і закінчуючи розробкою вдосконалених систем допомоги водієві. В даний час в автомобільній промисловості значний наголос приділяється розвитку систем взаємодії даних, інформації та розваг. Впершу чергу це спрямовано на підвищення безпеки подорожей, враховуючи вимоги водіїв відпочити та краще почуватися в поточних дорожніх умовах. Очікування автомобільного ринку щодо найближчого майбутнього зосереджені насамперед на напрямках підвищення стійкості до кібератак.

Слід підкреслити, що інтеграція автомобілів із системами Інтернету речей відповідно до концепції Industry 4.0 приносить багато нових можливостей, але також багато небезпек, до яких автомобіль повинен бути стійким. Прагнення до оптимізації витрат і повної автоматизації пов’язане з розвитком безпілотних автомобілів, які рухаються все швидше і швидше. Відповідно до бібліографії та оглядів автомобільного ринку основні цілі при розробці систем мехатроніки в автомобілях спрямовані на:

1. Автономне водіння, яке є одним із найзначніших досягнень мехатроніки. Мета полягає в тому, щоб створити можливість повністю автономного водіння, яке знаходиться на п’ятому рівні за п’ятибальною шкалою

автономності. В даний час деякі виробники починають тестування на третьому рівні автономності, тобто за певних умов водій може відмовитися від керування транспортним засобом, а підсистеми автомобіля контролюють його самостійно. Поспіх досягти все більшого й більшого рівня автономності також можливий завдяки швидкому розвитку мехатронних компонентів, таких як вдосконалені датчики (LiDAR, радар, камери), ефективні процесори та складні алгоритми керування. Вони дозволяють транспортним засобам здійснювати навігацію в реальному часі та приймати рішення без втручання людини. Досягнення повної автономності водіння, безсумнівно, революціонізує транспорт, зробивши його безпечнішим, ефективнішим і доступнішим для всіх завдяки можливості заміни водія алгоритмами[4].

2. Електрифікація та енергоефективність, яка пов’язана з необхідністю збільшити запас ходу, а отже, постачати все більше і більше енергії для електромобілів, що працюють від акумуляторів, а також гібридів. Це також фактор, який, безсумнівно, суттєво вплине на розвиток акумуляторних систем. Це передбачає необхідність постійного вдосконалення та інтеграції мехатронних систем. Системи керування батареями стають більш ефективними, оптимізуючи споживання енергії та розширюючи запас ходу електромобілів. Крім того, мехатроніка також відіграє ключову роль у розробці систем рекуперативного гальмування, роблячи автомобілі більш енергоефективними.
3. Прогнозне технічне обслуговування та моніторинг стану, що також пов'язано із застосуванням мехатронних систем. Вони дозволяють контролювати сам автомобіль у реальному часі та визначати технічний стан за допомогою датчиків і вбудованих процедур діагностики. Алгоритми прогнозованого технічного обслуговування аналізують дані та завчасно сповіщають водіїв про потенційні ризики та несправності, забезпечуючи своєчасний ремонт, мінімізуючи простої та підтримуючи автомобіль у найкращому робочому стані.

4. Кібербезпека та бездротові оновлення в автомобілях, які підключені до систем збору даних, також пов’язані з ключовою роллю мехатроніки. Цей аспект роботи автомобіля має забезпечувати надійну кібербезпеку. Проведення атаки на мехатронні системи управління може виявитися настільки проблематичним, що водій втратить здатність продовжувати рух. Слід підкреслити, що величезною загрозою є не тільки захоплення контролю, але й фактична дестабілізація штатної роботи автомобіля.

Передові методи шифрування та системи виявлення вторгнень будуть інтегровані в мехатронну архітектуру для захисту від потенційних кіберзагроз. Можливо, архітектура транспортного засобу розширена додатковими пристроями, які перевіряють, чи буде атака на комунікаційні шини. Зміна деяких параметрів мехатронних систем управління можлива за допомогою бездротового оновлення програмного забезпечення. Це дозволяє безперервно вдосконалювати та впроваджувати нові функції та засоби захисту без необхідності відвідування автосервісу.

1.2.1. Розвивиток технології дорожньої інфраструктури з використанням мехатронних підходів

Довгий час автомобільний транспорт базувався на подібних і незмінних засобах. Незалежно від того, чи йдеться про перевезення людей чи вантажів. Елементами транспортного середовища та інфраструктури, описаними в (Miyata, 2018), тобто водієм, автомобілем і дорогою, керували виключно люди. Швидкий прогрес у мехатронних технологіях, а також нові можливості інтеграції технологій відповідно до Industry 4.0 дозволили з’єднати елементи транспортного середовища з використанням підходів цифрового обміну даними [5]. В результаті інфраструктурою дорожнього руху можуть керувати не тільки люди, але й сучасні інформаційні технології, в тому числі методи на основі штучного інтелекту.

Таким чином, цифрова трансформація, яка є частиною четвертої промислової революції (Індустрія 4.0), принесла абсолютно нові можливості для автомобільного транспорту. Крім того, впровадження концепції Інтернету речей дозволило реалізувати багато функціональних можливостей, які значно

підвищують безпеку під час керування автомобілем та підвищують комфорт його використання.

Сьогодні, керуючи автомобілем, можна перевірити таку інформацію, як стан дороги, пробки чи зіткнення. Взаємодія систем і датчиків, якими оснащений автомобіль, дозволяє транспортному засобу швидко реагувати на різні ситуації, які можуть статися. Тому очікується вдосконалення та подальший розвиток усіх механізмів запобігання зіткненням. Пристрої та підходи, такі як радари чи камери, відомі давно, але зазвичай вони впроваджувалися локально та використовувалися для одного автомобіля. Ідея об'єднання всієї наявної дорожньої інфраструктури вносить суттєві зміни. Зібрану інформацію можна комбінувати та аналізувати разом, а потім використовувати в режимі реального часу для керування дорожнім рухом, як показано на рис. 1.8. Сьогодні ці автомобільні системи зв'язку розглядаються як частини більших екосистем, що відповідають ідеї Industry 4.0.

Рисунок 1.8. Огляд сценарію V2X за ідеями Industry 4.0

1.2.2. Кібербезпека в автомобільних вбудованих системах

Стійкість до кібератак в автомобільному секторі має вирішальне значення для захисту життів, особистих даних, функціональності автомобіля, репутації бренду, відповідності законодавству, фінансової стабільності та стійкості галузі. Іншими словами, необхідно розглянути всі можливі сценарії атаки та підготувати засоби

захисту від них. У розділі нижче описано, з якими типами атак ми можемо боротися з функціональної точки зору, наведено приклади успішних атак на транспортні засоби та описано захист від кібератак, який зараз використовується.

Приклад характеристик вбудованих систем наведено в (Ruiz, et al., 2012), де автори описують розробку цих систем на основі вбудованих компонентів. Удосконалення та впровадження таких систем є дуже складним завданням. Складність становить те, що вони розподілені і повинні працювати в режимі реального часу. З точки зору безпеки рівень зусиль, необхідних для того, щоб зробити вбудоване середовище стійким до загроз, також дуже високий. У згаданій статті обговорювалася методологія аналізу та моделювання загроз, що розуміються як атаки на системи, що складаються з вбудованих компонентів. Ключовим фактором є ідентифікація та класифікація загроз. Ключову роль відіграє модель порушника, яка дозволяє зрозуміти джерело ризику та запропонувати потенційні захисні дії, які є основою для визначення моделі загрози [6].

Автомобільна промисловість висуває додатковий рівень вимог, пов’язаних із повною безпекою транспортного засобу та забезпеченням захисту людей на найвищому можливому рівні. У статті (Gnacy–Gajdzik, Gajdzik, Przystałka, & Sternal, 2022) обговорюється необхідність впровадження стандарту ISO 26262. Відповідно до цього безпека системи досягається застосуванням різноманітних заходів безпеки. Одночасно це збільшує складність впровадження процесу безпеки для вбудованого дорожнього середовища. Хоча швидкий розвиток електроніки відкриває нові можливості, слід підкреслити, що наявні ресурси завжди цінні. Незважаючи на те, що для захисту можна використовувати все швидші процесори з більшими можливостями (наприклад, більше пам’яті або більше ядер для обчислень), ціна модуля все ще дуже висока. Це відіграє вирішальну роль через величезні обсяги виробництва.

Як зазначається (Desnitsky & Kotenko, 2014), специфіка вбудованого пристрою передбачає використання комбінованих механізмів захисту, що характеризуються належним рівнем безпеки та прийнятним споживанням

ресурсів. Тому доцільним виглядає подвійний підхід до проблеми. Це дає можливість використовувати складні та дорогі заходи безпеки, коли це критично, і недорогий метод, який підвищує рівень безпеки, коли цього достатньо.

Загрози можна класифікувати різними способами, відповідно до різних критеріїв. Орієнтовно, за походженням загроз їх можна поділити на зовнішні та внутрішні.

За функціональністю можна перерахувати підслуховування та перехоплення даних, дестабілізацію або спробу захоплення. Зразкова класифікація загроз була описана в (Rae & Wildman, 2003), де автори розділили їх за типами зловмисників.

Атаки, розглянуті з функціональної точки зору, було запропоновано розглянути таку класифікацію: прослуховування даних, запис даних і відтворення сценаріїв та атаки грубою силою.

1. Прослуховування даних

Цей тип атаки відносно простий у реалізації, оскільки не потребує додаткових обчислювальних потужностей виконавчої системи для обробки інформації за короткий час. Він полягає в підключенні до існуючої мережі за допомогою пристрою з сумісним інтерфейсом і прослуховуванні переданих даних. Більшість таких атак стосується бездротової передачі, оскільки вона передбачає відносно легкий фізичний доступ до мережі. Якщо передача не зашифрована, достатньо розмістити додатковий приймач модуля порушника (наприклад, з батарейним живленням) в зоні дії атакованої бездротової мережі, таким чином отримавши доступ до даних, що передаються. У літературі можна знайти різноманітні рішення для мінімізації ризику таких атак. У (Garnaev & Trappe, 2022) було розглянуто новий тип стратегії захисту від прослуховування. Основною метою підвищення рівня секретності було досягнення такого підходу у випадках найбільш непередбачуваних для супротивника шляхів.

Стаття (Zou & Wang, 2016) є прикладом опису оптимального датчика, який планує схему для захисту законної бездротової передачі від атак підслуховування. Датчик з найвищою секретністю планується передавати отриману інформацію до приймача. Автори (Das, Bhowmik, & Giri, 2017) стверджують, що підслуховування

є великою проблемою в бездротовій сенсорній мережі (WSN), яка споживає основну частину енергії. Таким чином, вони зосереджуються на розробці семантичного прослуховування преамбули для семантичної сенсорної мережі, щоб уникнути прослуховування. Вони пропонують онтологію для сенсорних вузлів і виявлених подій. У (Ndonda & Sadre, 2017) була описана стратегія багатошляхової маршрутизації. Він чергує кілька шляхів від вихідного хоста до кінцевого хосту. Цей підхід не може охопити всю комунікацію.

На жаль, це викликає критичні затримки. Автори також пропонують стратегію пріоритетної багатошляхової маршрутизації, яка дозволяє уникнути таких затримок. У (Wu, Jiang, Luo та Li, 2021) було представлено подвійний автоматичний кодувальник (DDAE). Він ґрунтувався на уніфікованій схемі (у сенсі спільного використання моделей DDAE) для захисту кіберфізичних систем (CPS) від прослуховування та виявлення типових атак, наприклад, атак із введенням помилкових даних (FDI), заперечення атаки з-під обслуговування (DoS) і атаки відтворення. Автори (Babaghayou, Labraoui, Ari, Ferrag, & Maglaras, 2020) зосереджуються на загрозах безпеці та конфіденційності, що виникають через технологію Internet of Vehicles. V2X дає багато прибутків, особливо зменшуючи кількість аварій, підключаючи автомобіль до дорожньої інфраструктури.

Тим не менш, як і кожна технологія, вона також має деякі слабкі місця, які необхідно захистити, див. рис. 1.9.

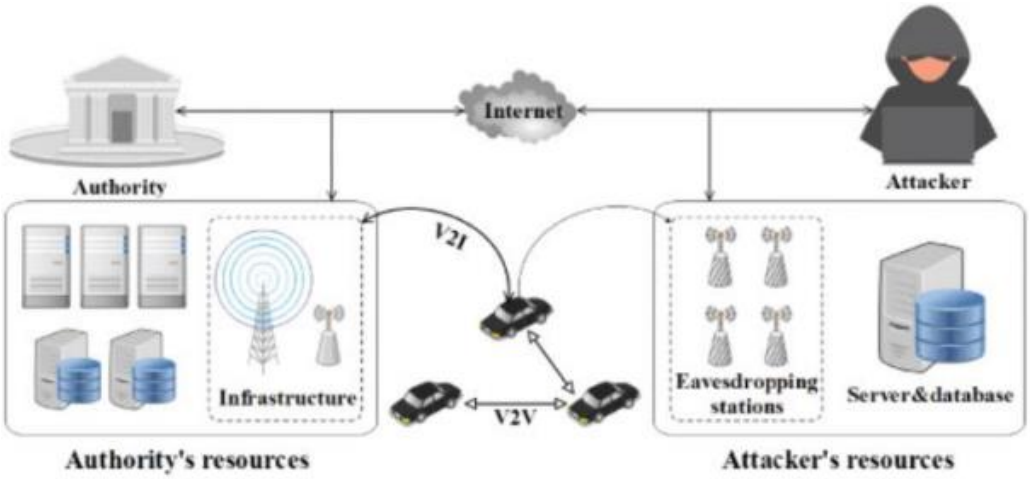


Рис.1.9. Сценарій прослуховування даних у V2X

2. Запис даних і відтворення сценаріїв

Дані, що надсилаються по CAN-шині, дуже часто не шифруються, зазвичай вони передаються відкрито. Причина полягає в тому, що шифрування на стороні відправника вимагає дешифрування на стороні одержувача, і тоді стягуються додаткові витрати на розробку. Слід зазначити, що це відповідає вимогам зворотної сумісності. Більш того, CAN найчастіше не захищений. Однак фрейми включені в безпечні операції. Наслідком відсутності шифрування є можливість взяти під контроль виконавчий модуль в автомобілі. Прикладом є прослуховування даних, що надсилаються на шину CAN. Тоді в момент їх активації використовується модуль порушника, тобто спрацьовування по шині.

Як підтверджено (Gajdzik, Timofiejczuk, & Sebzda, 2021), таким чином можна контролювати вмикання та вимкнення світлодіода. У випадку контрольного кадру E2E додатковою проблемою може бути правильне значення контрольної суми, обчислене на основі вмісту кадру та індексу. Для проведення успішної атаки необхідна синхронізація індексу, тобто збір даних для всіх 16 значень індексу (включаючи CRC) і їх повторення в належному порядку.

Таке рішення все ще не використовується, якщо його неможливо реалізувати та ефективно контролювати додаток. Як додатковий тип захисту, що мінімізує загрозу ризику, у (Gajdzik, Timofiejczuk, & Sebzda, 2021) запропоновано концепцію часового вікна. Рішення дозволяє підвищити безпеку передачі по шині CAN.

3. Атаки грубою силою

Ще один вид атаки, яка може становити серйозну загрозу здоров'ю та життю користувачів транспортного засобу, - це надсилання випадкових послідовностей даних на шину CAN. Може статися, що випадково надісланий набір бітів активує один з електронних модулів. З огляду на те, як працює CAN-шина, тобто кадри з певними ідентифікаторами надсилаються циклічно через певний проміжок часу (на практиці від 10 мілісекунд до кількох секунд), така атака займає багато часу.

Однак, враховуючи так звану інтелектуальну атаку грубим перебором, яка полягає в відправці підготовлених послідовностей даних (не всіх можливих бітових комбінацій), можна досягти успіху. Беручи до уваги сучасну

обчислювальну потужність виділених вбудованих систем, згідно з дослідженнями (Gillela, Prenosil, & Ginjala, 2019), безумовно, немає жодних обмежень щодо продуктивності для здійснення такого типу атак.

4. Методи зміни повідомлень шини CAN

Існує два варіанти підключення модуля охоронного пристрою до шини CAN в автомобілі:

• Модуль порушника підключається до шини CAN паралельно (пристрій має лише 1 інтерфейс шини CAN), див. рис. 1.10. Єдина можлива дія, яку можна виконати, полягає в читанні та надсиланні повідомлень CAN. Слід підкреслити, що немає можливості заблокувати передане повідомлення або замінити його вміст.

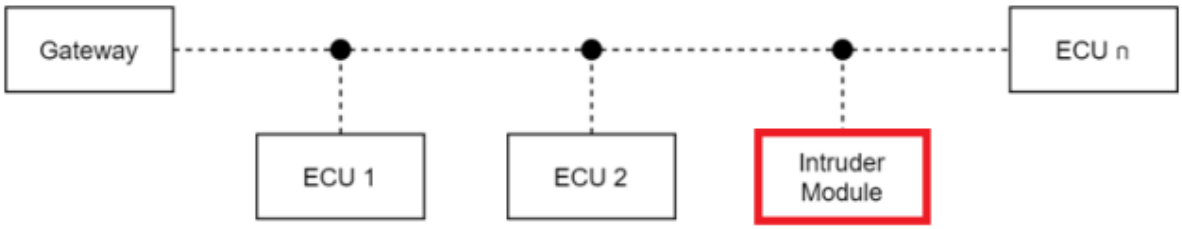


Рис.1.10. Intruder як паралельний модуль

• Модуль порушника підключається до шини CAN як міст (пристрій має 2 інтерфейси шини CAN), див. рис. 1.11. Обсяг можливих дій, які виконуються цими модулями: читання, надсилання, блокування та заміна вмісту повідомлень.

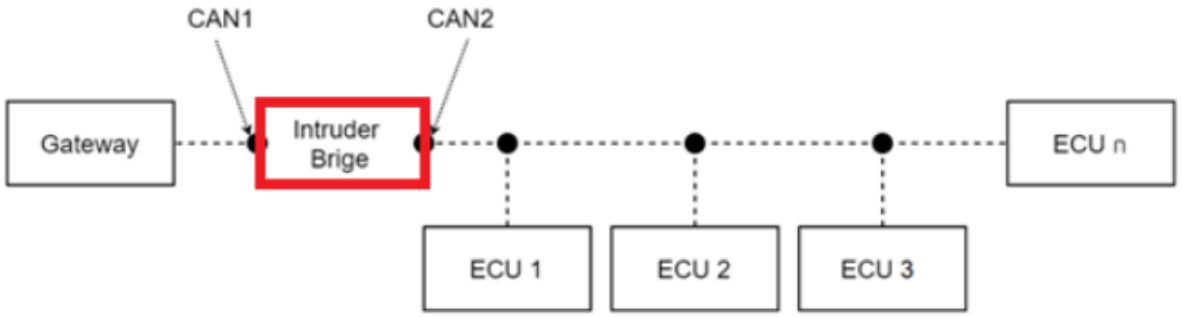


Рис.1.11. Порушник як міст

1.3. Вибрані застосування штучного інтелекту в автомобільній промисловості

Стрімкий розвиток алгоритмів і додатків штучного інтелекту (ШІ) спостерігається вже кілька років[7]. Штучний інтелект також має великий вплив на розвиток автомобільної промисловості через оптимізацію різних аспектів конструкції, виробництва, обслуговування та безпеки транспортних засобів. Особлива безпека є найважливішою темою, тому будь-які допоміжні функції на основі ШІ є ключовими. У (Halim, Kalsoom, Bashir, & Abbas, 2016) були представлені методи штучного інтелекту для безпеки водіння та прогнозування ДТП. Найпоширеніші застосування штучного інтелекту в автомобільній промисловості включають:

• Автономне водіння

Це найскладніша система управління, яка значною мірою спирається на алгоритми штучного інтелекту. Ці системи використовують такі пристрої, як датчики, камери, лідар і радар, щоб сприймати оточення та приймати рішення в режимі реального часу щодо безпечної навігації на основі поточних дорожніх умов навколо автомобіля.

• Розширені системи допомоги водієві (ADAS)

Такі функції ADAS, як адаптивний круїз-контроль, помічник у смузі руху та автоматичне екстрене гальмування, використовують алгоритми штучного інтелекту для підвищення безпеки та комфорту водія. Підходи штучного інтелекту дозволяють обробляти дані, зареєстровані датчиками, щоб забезпечити контроль над транспортним засобом за допомогою попереджень, що надаються водієві, і допомогти у разі небезпечних ситуацій на дорозі.

• Управління дорожнім рухом

Системи керування дорожнім рухом на основі штучного інтелекту допомагають зменшити затори та покращити транспортний потік, аналізуючи дані в режимі реального часу з дорожніх камер, пристроїв GPS та інших джерел для коригування дорожніх сигналів і маршрутів. Важливість цієї технології стрімко

зростає з розвитком систем, пов’язаних з автомобілями, відомих як «автомобілі для всього».

• Енергоефективність

Алгоритми штучного інтелекту оптимізують системи керування енергією для гібридних та електромобілів. Під час рекуперації вони керують процесом відновлення енергії. Під час заряджання вони визначають найкращі параметри, які дозволяють нам безпечно та відносно швидко зарядити батарею, а також забезпечити тривалий термін служби батареї.

• Прогнозне технічне обслуговування

Системи зв’язку із зовнішнім світом разом із підходами штучного інтелекту дозволяють обробляти дані, зареєстровані датчиками, розташованими в автомобілях. Результати обробки та аналізу даних дають інформацію про технічний стан автомобіля та його модулів. Постійний моніторинг деяких важливих параметрів дозволяє прогнозувати поломки, збої або необхідний час на технічне обслуговування. Такі підходи призводять до зниження витрат на обслуговування та збільшення часу безвідмовної роботи автомобіля.

• Обробка природної мови (NLP)

Голосові помічники, такі як Siri від Apple, Google Assistant і Alexa від Amazon, стають все більш популярними в автомобільній промисловості. Технологія NLP дозволяє водіям керувати різними функціями, такими як навігація, розваги та кондиціонування повітря, за допомогою голосових команд. Завдяки відсутності необхідності сенсорного керування шляхом фізичного натискання кнопки або сенсорного екрану, рівень безпеки під час водіння значно підвищився, оскільки водій може постійно стежити за ситуацією на дорозі поза транспортним засобом.

• Інформаційно-розважальна система та персоналізація

Інформаційно-розважальні системи на основі ШІ вивчають уподобання та поведінку водія, щоб пропонувати персоналізований контент і рекомендації. Вони допоможуть уникнути стресових ситуацій і покращать загальний досвід подорожі на автомобілі.

• Розпізнавання жестів і емоцій

Існує ряд додатків, заснованих на підходах штучного інтелекту, які можуть інтерпретувати жести та міміку водія та оцінювати швидкість і правильність реакції водія на дорожню ситуацію навколо транспортного засобу, щоб підвищити безпеку, розпізнаючи, коли водій сонливий або дратівливий.

• Кібербезпека

Зі збільшенням зв'язку автомобіля (V2X) методи штучного інтелекту відіграють ключову роль у виявленні та запобіганні кіберзагрозам, захисті систем автомобіля від вторгнень, що включають крадіжку даних, дестабілізацію руху або контроль над вибраним електронним модулем керування. Автори (Tong, Hussain, Bo, & Maharjan, 2019) зосереджуються на V2X разом із штучним інтелектом і розглядають різноманітні дослідження складних систем V2X.

Висновок до 1 розділу

Розділ описує процес проектування сучасного автомобіля. Опис базується на порівнянні з минулими підходами. Визначено напрямки розвитку автомобільних систем, які трансформувалися від механічних до мехатронних. У розділі перераховані потенційні небезпеки для систем автомобіля, як незахищені прогалини для кібератак. На основі проаналізованої літератури перераховано можливі типи кібератак, а також охарактеризовано приклади успішно проведених атак на автомобілі. Крім того, у цьому розділі розглядається література, щоб дослідити поточні заходи безпеки, що застосовуються в автомобілях.

РОЗДІЛ 2. АНАЛІЗ ФУНКЦІОНАЛЬНИХ ХАРАКТЕРИСТИК ТА ДОСЛІДЖЕННЯ ВБУДОВАНИХ СИСТЕМ У СУЧАСНИХ АВТОМОБІЛЯХ.

2.1. Багатофункціональний пристрій збору даних MicroDAQ E2000 із можливостями обробки в реальному часі

Серія E2000 призначена для програм збору даних і обробки в реальному часі. Завдяки виділеному ядру DSP користувач може виконувати код на незалежному процесорі. Серія E2000 ідеально підходить для програм управління та обробки сигналів [8]. Пристрій можна налаштувати з усіма доступними параметрами аналогового входу та виходу. Серія E2000 оснащена шістьма ШІМ-каналами, двома модулями кодування, до 32 цифрових каналів введення/виведення. Програмне забезпечення E2000 дозволяє використовувати пристрій з мовами програмування Scilab, Matlab/Simulink, LabView та C/C++ і Python(рис. 2.1.).

Рис.2.1. MicroDAQ E2000

Особливості

- Ядро DSP з фіксованою/плаваючою комою
- Ethernet і Wi-Fi
- Аналогові входи
- Аналогові виходи
- Цифрові входи та виходи
- UART, ШІМ, входи квадратурного кодера

Підтримувані операційні системи

- Windows/Linux/MacOS

- Підтримуване програмне забезпечення
- Scilab, MATLAB/Simulink,
- LabVIew, C/C++, Python

Специфікація MicroDAQ E2000 наведена в таблиці 1.

Таблиця 1. Специфікація MicroDAQ E2000

Блок обробки	Ядро DSP 300 або 456 МГц TI C674x з фіксованою/плаваючою комою
Пам'ять	до 32 ГБ пам'яті
Підключення	Ethernet 100Base-TX WIFI, IEEE 802.11n, роз'єм RP-SMA, 9dBi антена USB2.0 480MBit (пристрій зберігання даних)
Цифровий вхід/вихід	16 або 32 5-вольтових TTL/CMOS DIO з настроюваними функціями: • 6 ШІМ • 1 UART • 2 Модуль квадратурного кодера
Потужність	Джерело живлення 5 В постійного струму, живлення від USB - лише доступ до пам'яті
Робоча температура	від 0 °C до +70 °C (робочий), від -40 °C до +90 °C (тільки для зберігання)
Розміри	53,5x131x172 мм, 53,5x131x132 мм (конфігурація ADC01-DAC01)
Підтримка програмного забезпечення	**Scilab/Xcos** Набір інструментів MicroDAQ для Scilab - збір даних - автоматична генерація коду для DSP - інтеграція застарілого коду C - Підтримка доказів E4Coder **LabVIEW** • Обробка в реальному часі за допомогою MicroDAQ DSP • VI для: аналогового входу/виводу, DIO, Encoder, PWM, **UART** **Matlab/Simulink:** • Автоматична збірка та завантаження в ціль через Ethernet або WiFi • Підтримується автономний, PIL і зовнішній режими • Підтримка профілювання в режимі PIL • Бібліотека блоків Simulink

1. Аналоговий вхід

Аналогові входи MicroDAQ E2000 можна вибрати з десяти доступних варіантів. Користувач налаштовує MicroDAQ за допомогою рентабельних аналогових входів одночасної дискретизації та мультиплексування з частотою дискретизації до 2000 kps. Усі доступні параметри аналогового введення можна використовувати для збору даних і обробки в реальному часі.

2. Аналоговий вихід

Пристрій можна налаштувати з різними параметрами аналогового виходу. Від базової 100kps з вихідним діапазоном 0-5V до вдосконаленої 16-канальної, 16bit, 800ksps, ±10V, ±5V, ±2,5V, 0-10V, 0-5V багатодіапазонної опції. Усі доступні опції аналогового виводу можна використовувати для збору даних і обробки в реальному часі.

3. Ядро DSP

MicroDAQ E2000 оснащений процесором DSP. 300 або 456-МГц TMS320C674x з плаваючою/фіксованою точкою DSP може бути використаний для обробки сигналів і програм керування.

Програмне забезпечення MicroDAQ дозволяє використовувати DSP шляхом автоматичної генерації коду з Matlab/Simulink або Scilab/Xcos. Створену програму DSP можна завантажити через Ethernet або Wi-Fi на MicroDAQ DSP. Програмне забезпечення забезпечує доступ до даних програми в реальному часі під час виконання DSP.

4. Цифровий вхід/вихід

32/16 цифрових ліній введення/виведення налаштовані як 16/8 входів і 16/8 виходів. Лінії цифрового вводу/виводу спільно використовуються з ШІМ, входами кодувальника та портом UART. Цифровий вхід/вивід може використовуватися для збору даних або обробки в реальному часі під час виконання доступу з програми DSP.

5. Зберігання

MicroDAQ E2000 забезпечує до 32 Гб загальної пам’яті. Цю пам'ять можна використовувати для зберігання даних користувача. Користувач може

використовувати блок Simulink або Xcos «To File» для збереження даних із програми DSP. Доступ до пам'яті можна отримати через веб-браузер або USB.

6. Ethernet і Wi-Fi

Серія MicroDAQ E2000 забезпечує Ethernet і Wi-Fi. Обидва інтерфейси можна використовувати для керування пристроєм і обміну даними з головним ПК. Унікальні функції програмного забезпечення дозволяють завантажувати та отримувати доступ до даних програми під час виконання DSP через Ethernet або Wi-Fi.

2.2. PCAN-USB Pro. Інтерфейс CAN і LIN для високошвидкісного USB 2.0

Адаптер PCAN-USB Pro FD дозволяє підключати мережі CAN FD і LIN до комп'ютера через USB. Одночасно можна підключити дві польові шини, до чотирьох за допомогою відповідних адаптерних кабелів (2 x CAN FD, 2 x LIN) [9]. Кожен канал CAN FD окремо ізольований від USB і LIN з максимальною напругою 500 Вольт. Міцний алюмінієвий корпус робить адаптер PCAN-USB Pro FD придатним для мобільних додатків (рис.2.2.).

Рис.2.2. PCAN-USB Pro

Стандарт CAN FD (CAN з гнучкою швидкістю передачі даних) впершу чергу характеризується більшою пропускною здатністю для передачі даних. Максимально 64 байти даних на кадр CAN FD (замість 8 досі) можна передати зі швидкістю до 12 Мбіт/с. CAN FD сумісний зі стандартом CAN 2.0 A/B, тому вузли

CAN FD можна використовувати в існуючих мережах CAN. Однак у цьому випадку розширення CAN FD не застосовуються.

Програмне забезпечення монітора PCAN-View та інтерфейс програмування PCAN-Basic для розробки додатків із підключенням CAN входять до обсягу постачання та підтримки стандарту CAN FD. Програма для моніторингу PLIN-View Pro, а також інтерфейс програмування PLIN також входять до комплекту постачання.

1. ISO / Non-ISO CAN FD

З перших реалізацій CAN FD протокол був вдосконалений і тепер включений у стандарт ISO 11898-1. Переглянутий стандарт CAN FD не сумісний з оригінальним протоколом.

PEAK-System враховує це, підтримуючи обидві версії протоколу з їхніми інтерфейсами CAN FD. За потреби користувач може переключитися на протокол CAN FD, який використовується в середовищі програмним забезпеченням («Non-ISO» та «ISO»). Пристрої, поставлені до лютого 2015 року, потребують оновлення мікропрограми для цієї функції.

2. Особливості:
    - Адаптер для високошвидкісного USB 2.0 (сумісний з USB 1.1 і USB 3.0);
    - Передача та отримання повідомлень CAN FD та LIN за допомогою 2 з’єднань D-Sub (обидва з призначенням контактів для шини CAN FD та LIN);
    - Роздільна здатність мітки часу 1 мкс;
    - 5-вольтове живлення на роз’ємі D-Sub можна активувати за допомогою паяної перемички, наприклад, для зовнішнього перетворювача шини;
    - Живлення через USB;
    - Розширений діапазон робочих температур від -40 до +85 °C (від -40 до +185 °F).
3. Властивості роботи CAN:

- Відповідає специфікаціям CAN 2.0 A/B і FD;
- Підтримка CAN FD для стандартів ISO та не ISO з можливістю перемикання;
- Швидкість передачі даних CAN FD для поля даних (макс. 64 байти) від 25 кбіт/с до 12 Мбіт/с;
- Швидкість передачі даних CAN від 25 кбіт/с до 1 Мбіт/с;
- Реалізація FPGA контролера CAN FD;
- Трансивер NXP TJA1044GT CAN;
- Кожен канал CAN FD окремо опторозв'язаний від USB і LIN до 500 В;
- Термінатор CAN можна активувати за допомогою паяних перемичок, окремо для кожного каналу CAN;
- Вимірювання навантаження на шину, включаючи кадри помилок і кадри перевантаження на фізичній шині;
- Індукована генерація помилок для вхідних і вихідних повідомлень CAN.

4. Властивості роботи LIN:

- Бітрейт від 1 кбіт/с до 20 кбіт/с;
- Трансивер TJA1028 LIN;
- Сумісний з усіма специфікаціями LIN (до версії 2.2);
- Обидва канали LIN (загальна земля) опторозв’язані від USB і CAN FD;
- Може використовуватися як головний або підлеглий LIN (роздільна здатність головного завдання 1 мс);
- Автоматичне розпізнавання бітрейту, довжини кадру та типу контрольної суми;
- Автономний планувальник з підтримкою безумовних, подійних і спорадичних кадрів;
- Обладнання може працювати через таблицю розкладу (можна налаштувати до 8 таблиць розкладу із загальною кількістю 256 слотів).

5. Призначення контактів D-Sub(рис.2.3.):

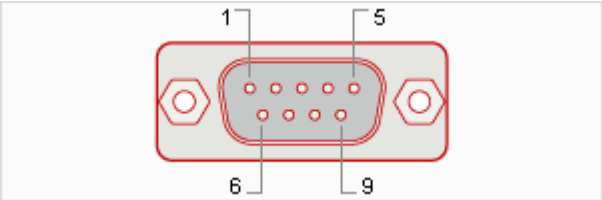


Рис.2.3. Призначення контактів D-Sub

- 1 Не підключено / опціонально +5 В
- 2 CAN-L
- 3 CAN-GND
- 4 LIN
- 5 LIN-GND
- 6 LIN-GND
- 7 CAN-H
- 9 VBAT

Висновок до 2 розділу

В даному розділі описано багатофункціональний пристрій збору даних MicroDAQ E2000 із можливостями обробки в реальному часі, розглянуто його особливості, специфікацію та підтримувані операційні системи. Також PCAN-USB Pro Інтерфейс CAN і LIN для високошвидкісного USB 2.0, наведені його особливості, властивості роботи та його призначення.

РОЗДІЛ 3. МЕТОДИ ОБРОБКИ БЕЗПЕКИ ВБУДОВАНИХ СИСТЕМ

3.1. Концепція часового вікна для пристроїв внутрішнього освітлення

Метою цього дослідження було порівняльне дослідження вразливості до атаки на виконавчий модуль, який керується шиною CAN FD [10].

Експеримент проводився за трьома сценаріями:

A. використання підходу часових вікон для встановлення дійсності сигналів;

B. використання передачі з наскрізним захистом;

C. з використанням стандартної передачі.

Поточне дослідження базується на застосуванні модифікацій програмного забезпечення. Програмне забезпечення характеризується дуже важливою перевагою, що дозволяє легко модифікувати та адаптувати до технологічних вимог. Оновлення програмного забезпечення значно дешевше в порівнянні з модифікацією апаратної структури.

Елемент, який зазнав атаки в цьому експерименті, позначено на рис. 3.1 і відповідає внутрішньому навколишньому освітленню.

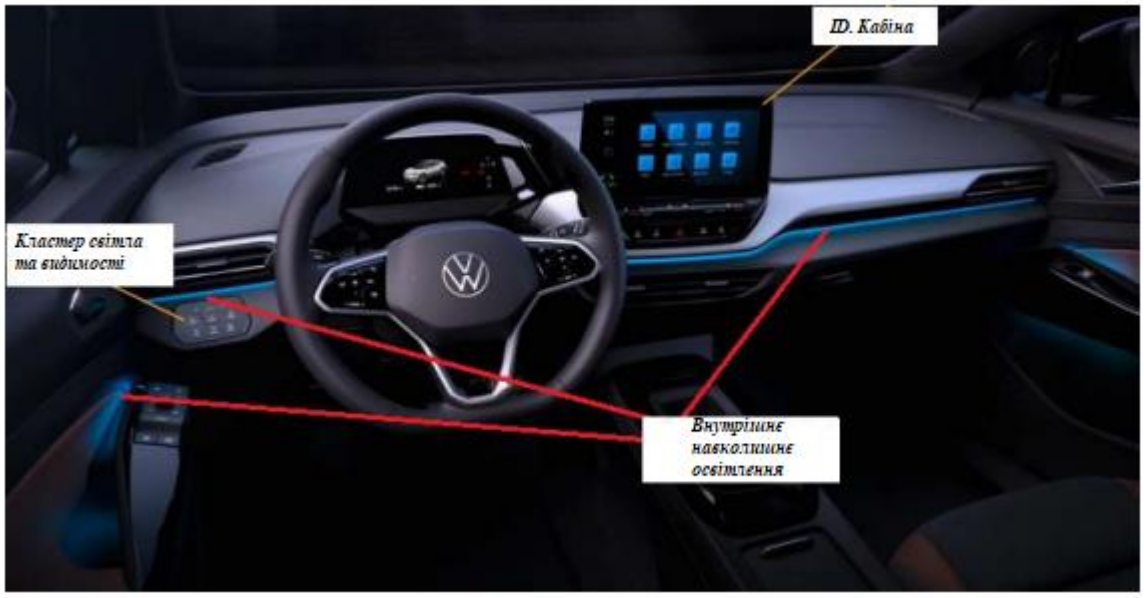


Рис.3.1. Внутрішнє навколишнє освітлення

В експерименті, атаку готували за допомогою методу відтворення раніше записаної передачі даних. Першим кроком є підключення до шини передачі даних додаткового пристрою, який може реєструвати кадри, відповідальні за управління даним модулем (наприклад, вмикання або вимкнення обраного світлодіодного

каналу) під час його штатної роботи. Потім записані сценарії відтворюються модулем порушника у вибраний момент, див. рис. 3.2. Очікуваним результатом є активація атакованого модуля після відтворення записаного речення даних.

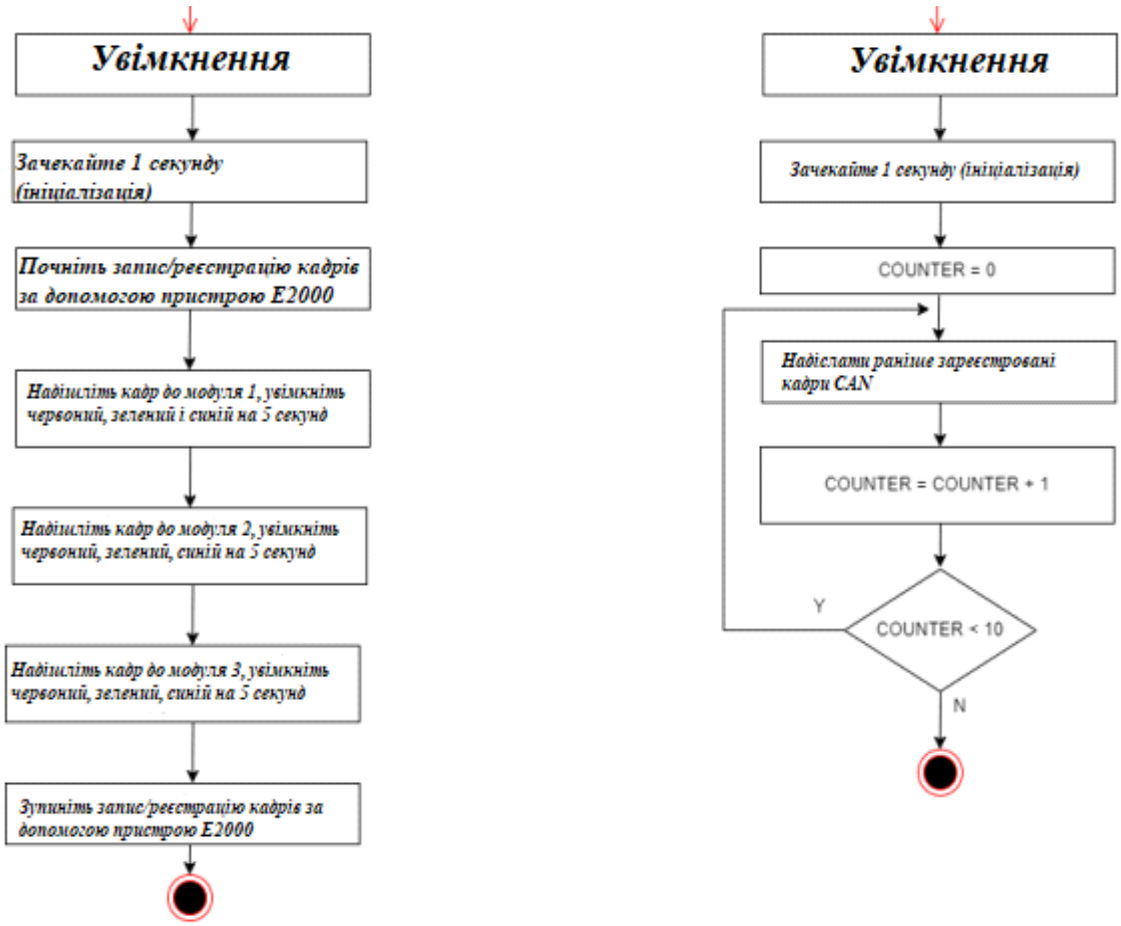


Рис.3.2. Алгоритм виконання атаки

Незалежно від обраного варіанту, в експерименті використовувався стандарт шини CAN FD. Це тому, що стандартний CAN характеризується надто коротким полем даних, щоб можна було розмістити всі необхідні керуючі сигнали в одному повідомленні.

Під час випробувань, проведених для варіантів B і C, використовувалася шина CAN FD з механізмом End-to-End protection (E2E). Забезпечує відповідний порядок доставлених рам. Це також означає, що пропуски кадрів усуваються, і легше виявити заміну бітів під час передачі. Запропонований підхід полягає в обчисленні контрольної суми з поля даних, починаючи з байта номер 1 (байт номер

0 містить інформацію про значення розрахованого CRC) на основі ключа, вбудованого в модуль.

Кожен виконавчий модуль зберігає 16 ключових значень залежно від поточного індексу, який змінюється від 0 до 15 відповідно до відношення індекс = (індекс+1) % 16. Алгоритм розрахунку CRC загальновідомий, тому, маючи достатньо велику кількість захоплень із шини даних (так званих журналів), можна розробити відповідне програмне забезпечення. Це програмне забезпечення відтворює 16 ключових значень для модуля. Однак слід зазначити, що механізм E2E не використовується для шифрування даних. Значення сигналу надсилаються відкрито, тому, підслуховуючи шину та аналізуючи поточний індекс, можна відправити раніше зареєстрований кадр із наступним індексом і атакувати виконавчий модуль. Метою представленого дослідження було перевірити стійкість до атак, що полягають у записі передач і подальшій відправці попередньо збережених кадрів на шину [11].

Перший етап перевірочних випробувань базувався на записі передачі по шині CAN під час штатної роботи, коли виконавчі модулі були активовані. Метою випробувань було визначити можливість успішної атаки типу кадрового сценарію. Кадри записувалися під час перемикання послідовних каналів світлодіодів у положення «ввімкнено» для всіх модулів, тобто першого червоного, зеленого та синього каналів. Час горіння діода, підключеного до певного каналу, становив близько 5 секунд. Потім після вибору кадрів з певного часу вони відтворювалися і відправлялися в шину. Предметом спостереження було перевірити, чи можливо контролювати необхідний модуль шляхом повторного відтворення раніше записаних кадрів у 4 випадках: при відтворенні повної послідовності записаних кадрів і 75%, 50% і 25% записаних кадрів, надісланих під час оригіналу. Кожен тест проводили 10 разів.

Випробування проводилися для 3 різних варіантів трансмісії CAN:

A. передача по шині CAN FD, довжина поля даних 24 байти, без додаткового захисту під час передачі;

B. передача по шині CAN FD, довжина поля даних 24 байти, захист End-to-End, тобто механізм захисту від втрати кадру або зміни значення сигналів у кадрі;

C. передача по шині CAN FD, довжина поля даних 24 байти, захист End-to-End з додатковим механізмом визначення дійсності сигналів в певний час (TW - time window). Тривалість дії вікна часу була встановлена на 100 мс.

3.2. Ін'єкційна діагностика

Метою даного експерименту було проаналізувати можливість проведення повної діагностики модуля автомобіля під час його штатної експлуатації, тобто в реальних умовах. Передбачалося, що для отримання визначених умов тестування необхідно вводити інформацію та замінювати її в захоплених кадрах CAN у реальному часі. У проведених дослідженнях використовувався механізм фіксації ключових сигналів з точки зору діагностики, зчитування значень змінних із збереженням вихідних часових циклів. Завдяки механізму фіксації інформації та її запуску в певний час, а потім зчитування через спільну пам’ять, була усунена необхідність розширення комунікаційної матриці з подальшими повідомленнями налагодження, які б збільшували ступінь зайнятості шини. Атаковані елементи автомобіля показані на рис. 3.3. і відповідають гальмівній системі [12].

Рис.3.3. Гальмівна система

Експеримент мав на меті перевірити, чи можливий обмін сигналами всередині CAN таким чином, щоб він був невидимим для автомобіля, який проходить процедуру діагностики. Дослідження було розділено на 2 етапи.

Тривалість кожного сеансу становила 2 хвилини і повторювалася 3 рази. На першому етапі (див. рис. 3.4.) було перевірено, чи можливий одночасний обмін сигналами у більшій кількості кадрів по CAN-шині у спосіб, непомітний для автомобіля під час зчитування діагностичних параметрів. Проведений тест включав поточне зчитування параметрів у кадрі, що містить інформацію про поточний тиск у гальмівній системі. Діагностичні дані, отримані від пристрою, безпосередньо оброблялися та перетворювалися на графік. Такий підхід дозволяє спостерігати та аналізувати сигнали в реальному часі. Водночас під час діагностики було експериментально перевірено максимальну кількість кадрів, які можна замінити в режимі реального часу, щоб це не було виявлено системою автомобіля. Випробування планувалися для обміну сигналами в 1, 5, 10, 15 і 20 кадрах CAN.

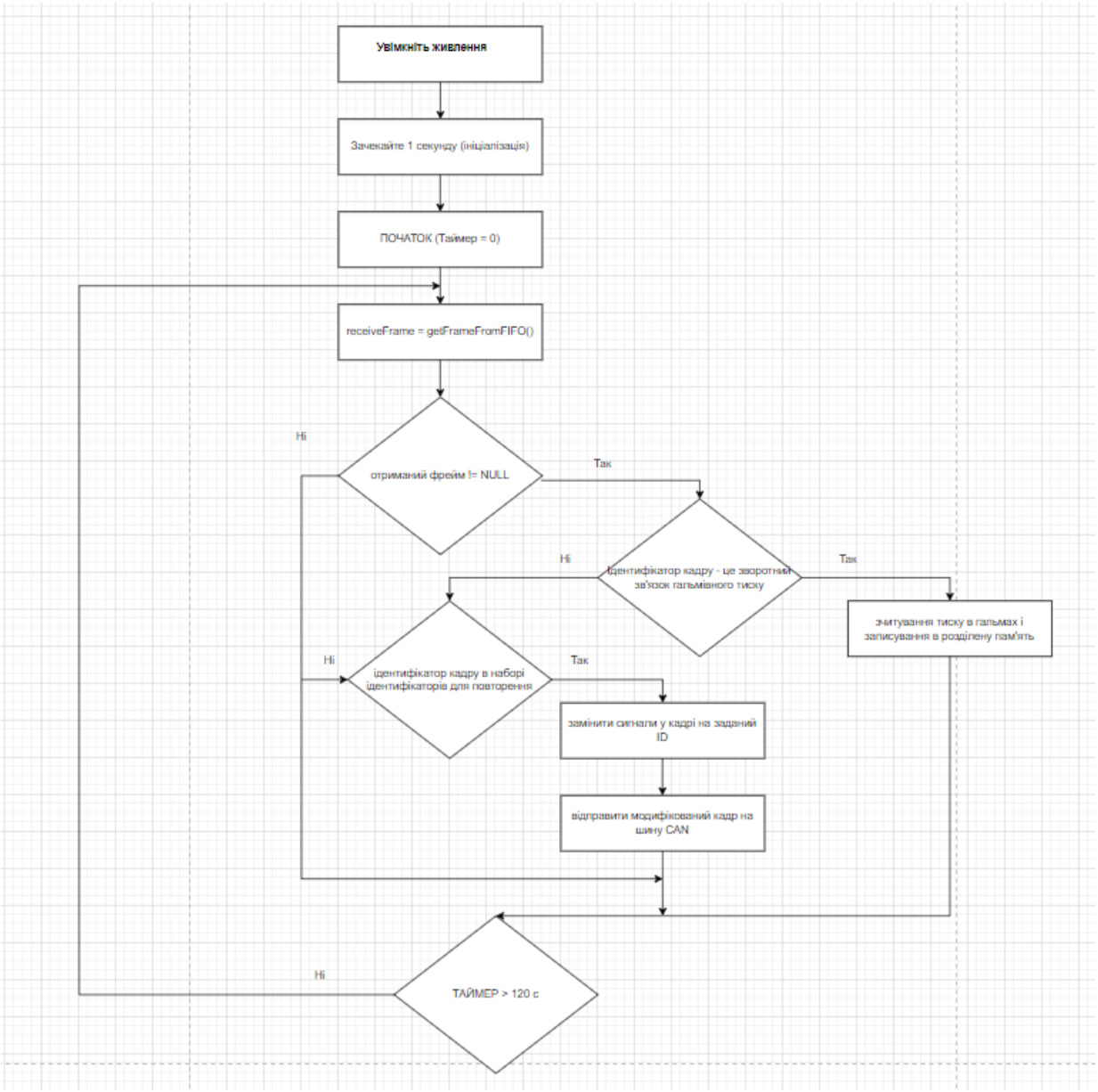


Рис.3.4. Структурна схема першого етапу експерименту

На другому етапі експерименту (див. рис. 3.5.) було перевірено, чи можна прочитати будь-яку інформацію, що міститься в CAN-кадрах, з конкретними ідентифікаторами та замінити значення бажаного сигналу, коли цього вимагає діагностична процедура. Оскільки в поточному кадрі CAN надсилає лише інформацію про поточний стан сигналу, іноді необхідно було зафіксувати значення сигналу в пам’яті модуля, щоб використовувати їх у потрібний момент. Ця функція була доступна, оскільки використовувалися так звані тестові точки програмного забезпечення. Під час випробувань механізм спільної пам'яті використовувався як механізм зв'язку між пристроєм, що піддається діагностиці, і

комп'ютером. Обмін інформацією за допомогою пам'яті та подальший зв'язок через інтерфейс Ethernet, двостороння передача даних дозволили здійснити атаку таким чином, що практично не вплинуло на час і завантаження CAN-шини додатковими діагностичними повідомленнями [13].

У тесті встановлювалися значення витрати для головного гальмівного циліндра (заміна значень контролю сигналу разом з розрахунком контрольної суми для всієї рами) і одночасно зчитувалися параметри поточного тиску в гальмівній системі. Крім того, були замінені кадри з наступними ідентифікаторами, що містять раніше захоплені значення сигналу. Випробування заміщення сигналу проводилися для: 1, 5, 10, 15 і 20 CAN кадрів.

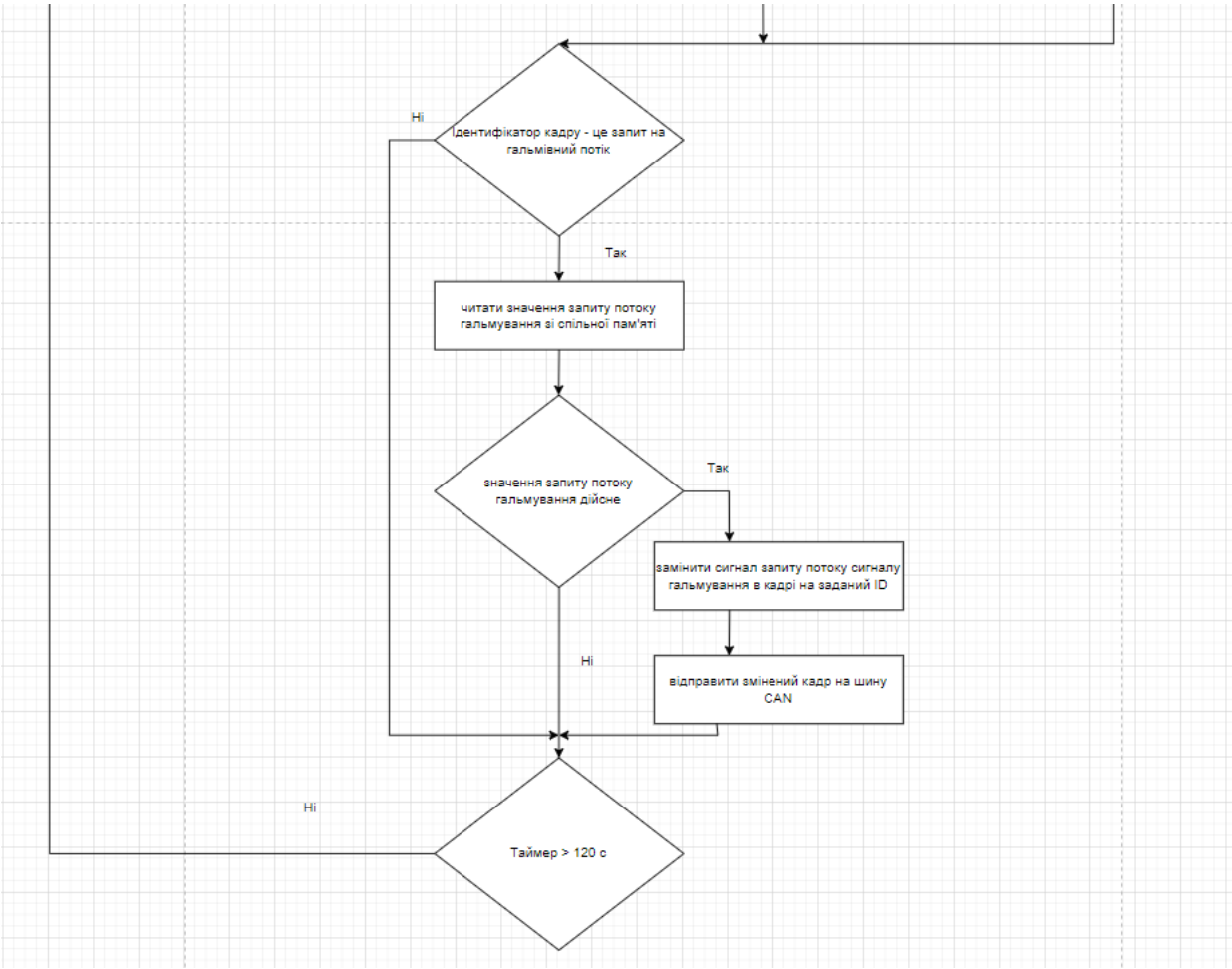


Рис.3.5. Структурна схема другого етапу експерименту

Дослідницьке середовище / випробувальний стенд.

Впровадженню процедур діагностики піддали справжній електромобіль. Тому необхідно було підготувати точки входу в систему зв'язку між електронними блоками управління за допомогою CAN-шини. Найкраще місце для всіх шин CAN – це шлюз. Це причина, чому його було видалено та підключено до решти тестової системи за допомогою додаткових кабелів і адаптерів (показано на рис. 3.7). Оскільки випробування проводилися під час штатної експлуатації автомобіля, необхідно було дотримуватися дуже жорстких часових вимог для обробки інформації, яка підлягає обміну, і зчитування статусу параметрів. Важливо було не привести перевірену електронну систему в стан помилки. Тому надзвичайно висока ефективність спеціального обладнання стала критичним параметром. Під час підготовки до випробувань було оцінено, що під час маніпулювання переданими сигналами час між останнім байтом отриманого оригінального кадру та останнім байтом модифікованого кадру повинен бути менше однієї мілісекунди. Це пов'язано з архітектурою сучасних ECU (Electronic Control Unit), чиї операційні системи з точки зору графіків працюють з роздільною здатністю 1 мілісекунда.

Така висока продуктивність також необхідна через необхідність модифікувати сигнали, що містяться в кадрі CAN, і перерахувати контрольну суму, необхідну в механізмі End-to-End Protection (E2E). Під час діагностичних досліджень використовувався пристрій MicroDAQ E2000 (рис. 3.6.), який відповідає вищезазначеним вимогам. Він оснащений двоканальним зв'язком CAN FD з підтримкою конвеєра багатоядерної обробки. Крім того, він пропонує інтерфейси Wi-Fi та Ethernet, які використовувалися для передачі двосторонньої передачі діагностичних сигналів. Завдяки цьому рішенню вихідний зв'язок між модулями на шині CAN не був порушений або будь-яким чином змінений. Крім того, процес читання значень «зафіксованих параметрів» також використовує прямий доступ до спільної пам'яті, що є найшвидшим можливим рішенням.

Пристрій MicroDAQ E2000 було підключено послідовно до шини № 4, відповідальної за гальмівну систему та рульовий механізм, як показано на рис. 3.6. Реальне підключення пристрою Microdaq E2000 до системи автомобіля показано на рис. 3.7.

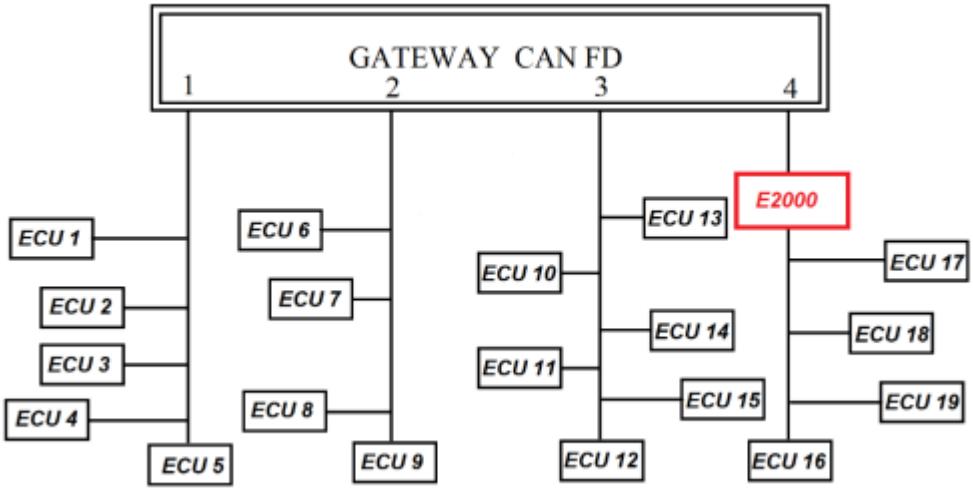


Рис.3.6. Схема тестованої системи

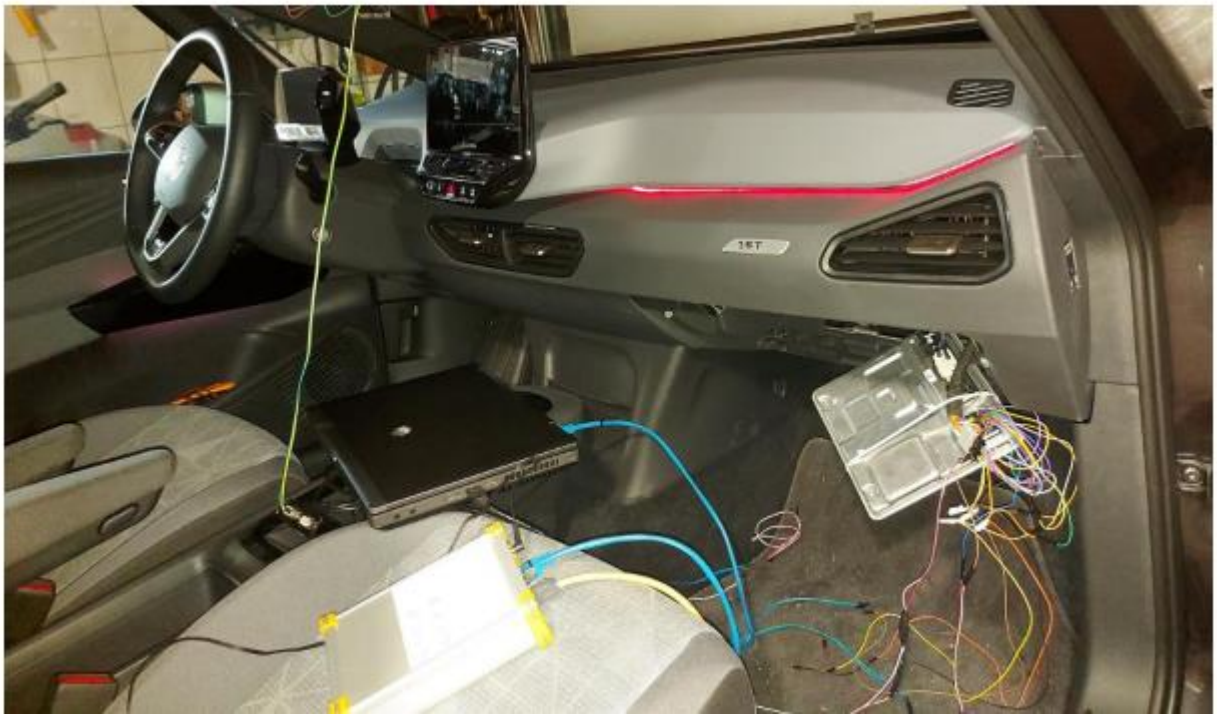


Рис.3.7. Підключення пристрою Microdaq E2000 до системи автомобіля

3.3. Експериментальна діагностика проведення кібератаки

Основною метою дослідження, проведеного в рамках цього експерименту, було продемонструвати, що можна успішно атакувати електронний модуль в автомобілі. Метою було взяти під контроль задній поворотник. Це було зроблено шляхом маскування представленої інформації до водія. Таким чином, водій, увімкнувши індикатор, бачить очікуваний стан на дисплеї, а задня мигалка не працює. Крім того, запропоновано оригінальну концепцію реалізації додаткового

недорогого захисту систем передачі даних. Було суттєво утруднено цей вид атаки, а потім перевірено ефективність його роботи. Запропоноване рішення базується на програмному підході до теми шифрування без використання спеціальних апаратних модулів, що, крім того, зменшує вартість впровадження, а також забезпечує легку модифікацію та адаптацію до технологій, що швидко змінюються. Атакований елемент у цьому експерименті позначено на рис. 3.8 і відповідає задньому поворотнику.

Рис.3.8. Задній поворотник

Дослідження, проведені в ході експерименту, було розділено на кілька етапів. Основна мета полягала в тому, щоб довести, що можна взяти під контроль транспортний засіб, не маючи документації з детальним описом інформації, що міститься в переданих кадрах CAN. Усі керуючі сигнали потрібно було знайти заздалегідь. Це було зроблено за допомогою власних методів зворотного проектування. Метою нападу став задній поворотник електрокара. Більше того, здійсненню такої атаки завадило додаткове припущення, що за сигнал відповідає задній поворотник. Під час атаки його робота неактивна, а водій постійно бачить статус на дисплеї, що підтверджує правильність роботи мигалки. Експеримент також доводить, що великою загрозою є не лише контроль над основними механізмами транспортного засобу, такими як прискорення, гальмування чи поворот. Кожне захоплення контролю над модулем автомобіля може призвести до

непередбачених наслідків [14]. Застосований підхід, представлений на рис. 3.9., означає, що в разі успішної атаки навіть на контрольний сигнал поворотників результат може бути катастрофічним. Водій автомобіля № 2, наближаючись до автомобіля червоного кольору, який стоїть на узбіччі, намагається його оминути, вмикає лівий покажчик повороту та, переконавшись, що сигналізує поворот ліворуч, виїжджає на дорогу автомобіля № 1, який їде в лівій смузі. Під час виконання маневру повороту водій не знає про поточну атаку (що задні покажчики повороту не працюють), оскільки йому відображається правильний статус.

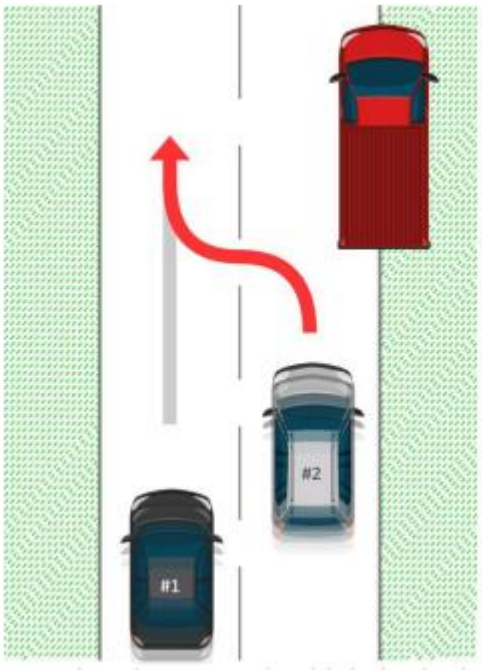


Рис.3.9. Об'їзд зупиненого автомобіля по лівій смузі

Перший етап експерименту полягав у зборі відповідної кількості даних з CAN-шини, коли потрібна функція не активна, тобто покажчики повороту вимкнені. У той час були записані дані, які також включали сигнали, що відповідають за керування покажчиком повороту, коли він неактивний. У дослідженні використовувався метод, представлений на рис. 3.10., який дозволив визначити кілька ідентифікаторів CAN-кадрів, які могли б відповідати за керування покажчиком повороту.

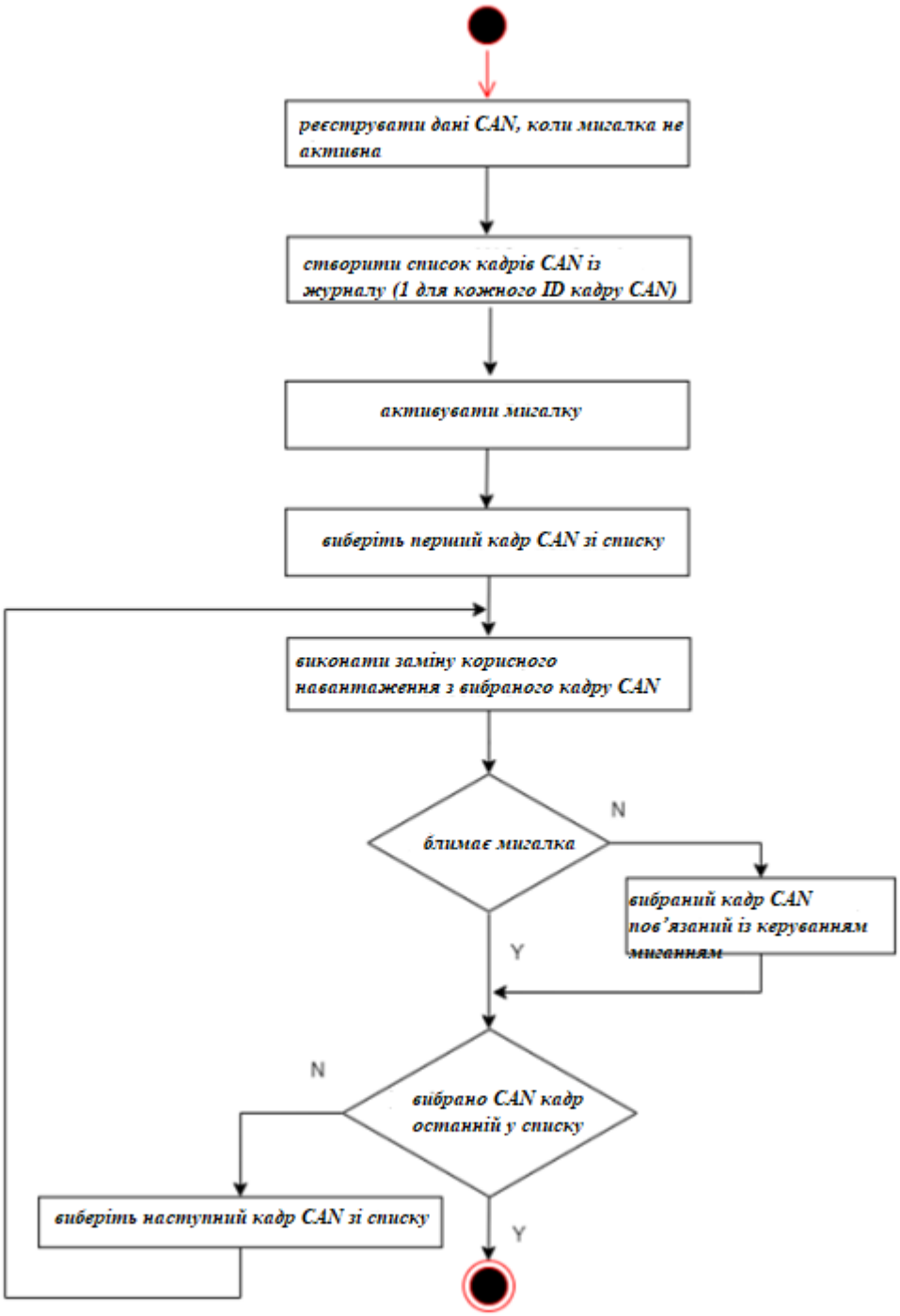


Рис.3.10. Блок-схема методу дослідження пошуку ідентифікаторів CAN

Потім із раніше зареєстрованих кадрів CAN для кожного ідентифікатора було обрано один кадр. Таким чином був створений список кадрів CAN, які використовувалися для заміни активного сигналу. Для кожного заміненого кадру спостерігалося, чи перестане працювати мигалка і чи це було виконано. Це

причина кваліфікувати ідентифікатор даного кадру CAN до набору кадрів, відповідальних за керування покажчиком повороту. Однак, щоб зробити можливим заміну кадрів CAN за допомогою пристрою MicroDAQ E2000, підключеного послідовно до шини в режимі моста, необхідно було розкодувати ключі механізму End-to-End Protection (E2E). Оскільки метод захисту E2E не використовується для шифрування даних, а його завдання – контролювати правильність потоку кадрів CAN, алгоритм розрахунку CRC є загальновідомим. Таким чином, вдалося знайти ключові значення за допомогою методу зворотного проектування та реалізації програми, що використовує грубу силу. Для цього було перевірено всі можливі значення ключів, на їх основі розраховано контрольну суму CRC і порівняно з контрольною сумою, збереженою в журналах. Якщо значення CRC збігалися, це означало, що ключ знайдено. Пошук ключів тривав, поки не було знайдено 16 ключових значень для індексів від 0 до 15. Весь процес показано на рис. 3.11[15].

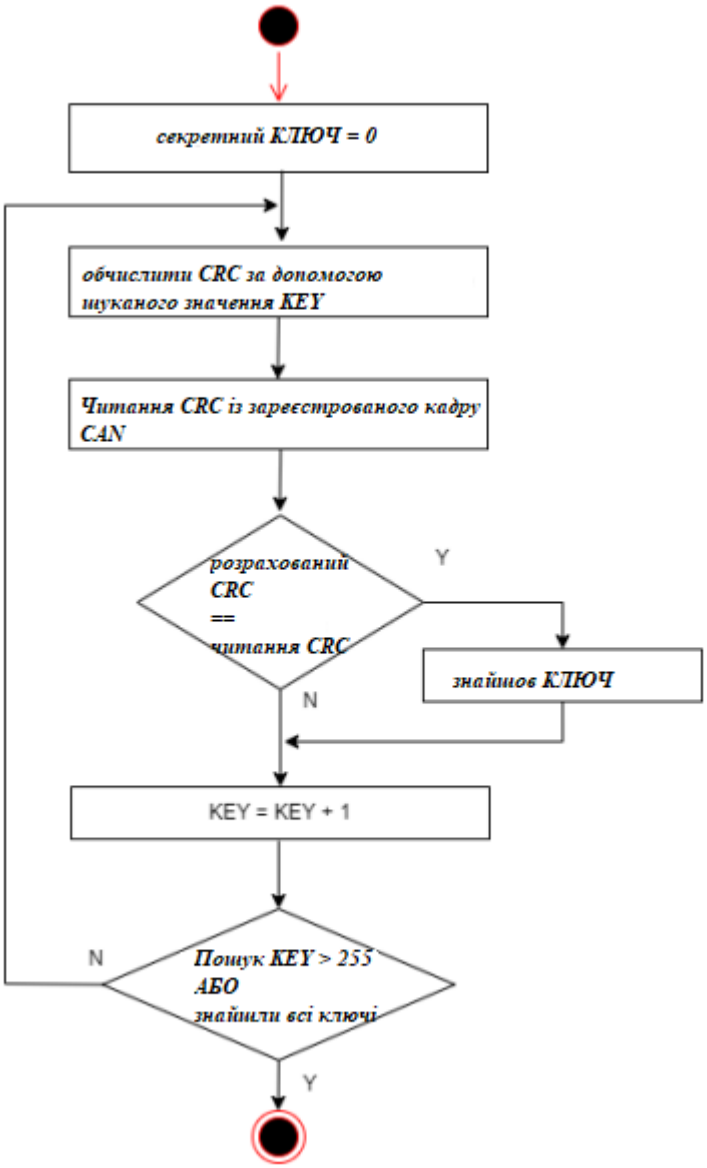


Рис.3.11. Блок-схема алгоритму пошуку ключів E2E

Нарешті, зібравши всі потенційні CAN-кадри, відповідальні за керування мигалками, необхідно було декодувати сигнали (послідовні окремі біти) всередині CAN-кадрів, відповідальних за керування мигалками. Для цього була створена концепція теплової карти для візуалізації графічного представлення бітів на осі часу. На вертикальній осі вказано час, а на горизонтальній осі – усі біти в кадрі CAN. Отже, як результат було запропоновано концепцію графічного перегляду для всіх бітів за певний час, де білі пікселі представляють бітове значення, що дорівнює 0, а чорні пікселі представляють бітове значення, що дорівнює 1.

Зразкова концепція теплової карти показана на рис. 3.12.

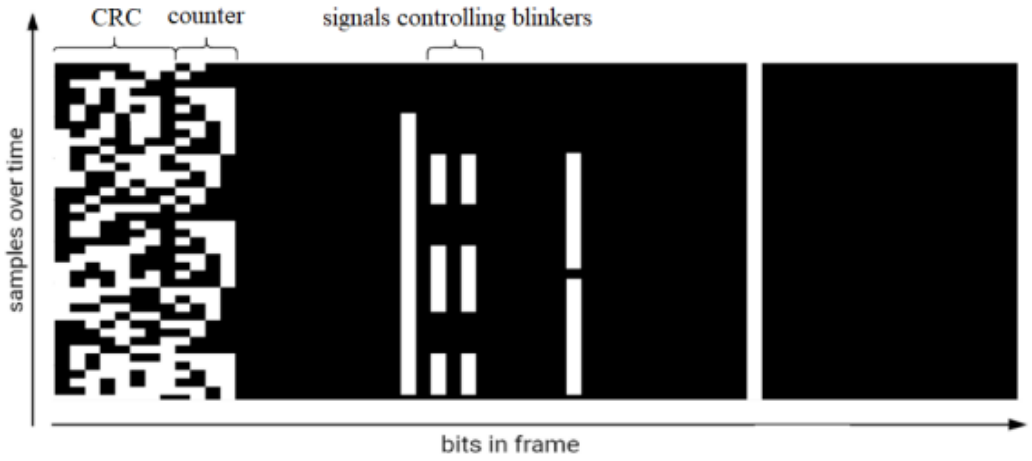


Рис.3.12. Візуалізація стану бітів із захистом E2E

Останній етап експерименту полягав у перевірці ефективності запропонованого недорогого методу програмного шифрування вмісту кадру CAN. Цей підхід передбачає виконання операції XOR над даними, що передаються в CAN-кадрах, з наголосом на двічі виконання операції XOR для залежності. На основі цих операцій отримується початкове значення. Основна мета запропонованого методу полягає в тому, щоб ускладнити декодування керуючих сигналів, наприклад, за допомогою методів, представлених раніше в цьому експерименті. Оскільки дослідження та випробування проводилися на електромобілі, придбаному в автосалоні, а не на тестовому прототипі, модифікувати програмне забезпечення, реалізоване в модулях управління, було неможливо. Таким чином, моделювання було зроблено шляхом додавання 2 модулів до системи: кодера та декодера. Слід підкреслити, що такий самий ефект було отримано, якщо шифрування було виконано в модулі, що передає повідомлення, і дешифрування на модулі-одержувачі.

Дослідницьке середовище / випробувальний стенд.

Отже, об’єктом випробувань був реальний автомобіль, необхідно було підготувати точки підключення до системи зв’язку між електронними блоками управління за допомогою шини CAN. Як було описано вище, під час випробувань пристрій мав замінити CAN-фрейми. Один із автобусів, що прямував прямо з головних шлюзів, підрізали. При цьому пристрій, що працює в режимі мосту, було підключено до системи зв’язку автомобіля, як показано на рис. 3.13.

Рис.3.13. Реальний автомобільний пристрій Microdaq E2000 як міст, підключений до шини CAN

Перший етап дослідження полягав у реєстрації передачі при вимкненому поворотнику. Процес реєстрації проводився за допомогою стандартного пристрою PCAN-USB PRO (показано на рис. 3.14), доступного на ринку. Отримані дані були

збережені на жорсткому диску комп’ютера (приклад часткового вмісту журналу наведено на рис. 3.15.).

Рис.3.14. 2-канальний пристрій CAN FD PCAN-USB PRO

```
Lister - [d:\SVNs\SNV_Kamil_ID_3\01_05_Traces\2021-01-03\kierownica7_8.trc]
File  Edit  Options  Encoding  Help
;$FILEVERSION=2.0
;$STARTTIME=44199.7682994987
;$COLUMNS=N,O,T,I,d,l,D
;
;   Start time: 03.01.2021 18:26:21.076.0
;   Generated by PCAN-View v4.3.0.596
;-------------------------------------------------------------------------------
;   Connection                Bit rate
;   PCANLight_USB_15@pcan_usb  Nominal 500 kBit/s, Data 2 MBit/s
;-------------------------------------------------------------------------------
;   Message   Time    Type ID     Rx/Tx
;   Number    Offset  |    [hex]  |  Data Length
;   |         [ms]    |    |      |  |  Data [hex] ...
;   |         |       |    |      |  |  |
;---+-- -----+------- +- --+----- +- +- +- -- -- -- -- -- -- -- --
     1         0.354 FB 12DD54E9 Rx 8  00 00 00 00 00 00 00 00
     2         0.465 FB      089F Rx 8  D0 07 89 00 00 12 80 F0
     3         2.195 FB      08AD Rx 8  02 E8 BF FF 00 1A 00 00
     4         2.464 FB      0886 Rx 8  00 00 CE 00 00 00 00 00
     5         4.737 FB      0592 Rx 8  00 00 00 00 00 00 00 00
     6         4.849 FB      03DB Rx 8  D4 03 00 00 00 00 00 7C
     7         5.151 FB      013D Rx 32 3F 17 11 11 01 94 03 00 00 00 70 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
     8         5.734 FB      0102 Rx A8 57 0D 7E FB 01 02 40 10 00 00 09 A5 02 00 00 30 00 00 00 00 00 00 EC 1F 00 00 00 00 00 24 D4 FF 31 00 20 A6 00 00 00 00 20 01 00 00 00 00 00 00 00
     9         6.027 FB      08FC Rx A8 9B B6 31 00 7E 18 93 10 00 00 00 00 00 00 00 00 00 10 2B 2B 21 21 09 00 00 00 00 00 00 00 00 00 00 00 00 F4 01 A0 FF EB 7F 38 C8 EA 81 AF AE 1E
    10         6.138 FB      012B Rx 8  8D 43 80 30 00 00 00 00
    11         6.250 FB      08FD Rx 8  AD DD 1F 81 00 00 00 00
    12         6.362 FB      0116 Rx 8  68 0D 00 00 00 00 00 FF
    13         6.589 FB      0139 Rx 32 02 0D 95 00 00 00 11 20 00 90 22 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
    14         6.827 FB      08C0 Rx 32 C9 8A FE E7 7F 10 27 93 E6 7F FF F3 3F FF F3 3F FC 0F 00 00 C0 FF FE 07 00 00 00 00 00 00 00 00
    15         7.446 FB      0086 Rx 8  64 01 CE 00 00 00 00 00
    16         9.020 FB      0040 Rx 8  A6 BF 00 80 00 00 15 87
    17         9.525 FB      0105 Rx 8  69 2E 10 00 30 02 C0 02
    18         9.638 FB      08C9 Rx 8  F8 00 00 00 00 FE 00 C0
    19        10.383 FB      089F Rx 8  92 08 89 00 00 12 80 F0
    20        11.600 FB      026B Rx 8  AB 01 00 00 00 00 00 00
    21        11.979 FB      0183 Rx 64 00 00 00 00 00 00 00 00 0E 80 00 00 80 FF 00 00 00 80 00 00 80 FF 00 00 31 00 00 A4 00 73 00 00 00 00 80 FF 07 80 80 00 00 00 80 FF 07 80 80 00 00 BC 19 95 40 29 7B 80 2F
    22        12.365 FB      023A Rx 64 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 A0 0F C4 00 00 00 00 00 00 00 00 88 F3 28 23 00 00 00 00 00 00 28 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00
    23        12.476 FB      0086 Rx 8  C8 02 CE 00 00 00 00 00
    24        12.587 FB      08AD Rx 8  A6 E9 BF FF 00 1A 00 00
    25        13.271 FB      020A Rx 64 75 F6 3F FD 25 00 08 10 00 E8 7E 37 B8 20 83 7E 00 7D 40 1F 00 FC 7F 64 FE FF 7F 0D 20 EE 64 08 80 C2 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
    26        13.497 FB      0108 Rx 32 A5 0D 00 00 00 00 7E FE 00 00 00 00 00 0A FF 01 00 00 00 00 00 00 00 00 00 00 00 00 00 90 24 00
    27        14.762 FB      03D6 Rx 8  00 00 00 00 00 00 00 00
    28        15.090 FB      013D Rx 32 F6 18 11 11 01 94 03 00 00 00 70 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
    29        15.318 FB      01AD Rx 32 B8 01 00 FE 07 00 00 08 FE 07 FE 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 09 00 3F
    30        15.611 FB      08FC Rx A8 D5 BB 31 00 7E 18 93 10 00 00 00 00 00 00 00 00 00 10 2B 2B 21 21 09 00 00 00 00 00 00 00 00 00 00 00 00 F4 01 A0 FF EB 7F 38 C8 EA 81 AF AE 1E
    31        15.987 FB      024F Rx 64 00 00 81 00 0C 00 E0 14 A1 D0 1F 80 54 F0 1F 80 00 00 00 00 74 68 1D 80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
    32        16.098 FB      0656 Rx 8  BC 0D 00 00 00 00 00 00
    33        16.405 FB      0300 Rx A8 00 00 00 00 00 00 00 00 00 00 00 00 00 F0 3F 00 23 00 00 00 00 F0 7F 37 FF FF 00 00 80 00 00 00 00 00 00 FF 7F 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
    34        16.854 FB      08C0 Rx 32 B6 85 FE E7 7F 10 27 93 E6 7F FF F3 3F FF F3 3F FC 0F 00 00 C0 FF FE 07 00 00 00 00 00 00 00 00
    35        17.448 FB      0086 Rx 8  AC 03 CE 00 00 00 00 00
    36        18.340 FB      020B Rx 8  FF 3F E0 07 02 EE BF FF
    37        18.529 FB      0206 Rx 24 BA EA 7E 80 00 F8 0F 7A 00 00 00 00 00 00 00 00 01 FB FE 03 00 00 00 10
    38        19.788 FB      0397 Rx 8  00 80 10 00 50 FA 3E 00
    39        20.326 FB      0318 Rx 8  00 00 0E BF FE 03 00 00
    40        20.437 FB      089F Rx 8  F6 09 89 00 00 12 80 F0
    41        20.727 DT 1B00004F Rx 8  00 00 00 04 01 00 00 00
```

Рис.3.15. Приклад часткового вигляду файлу журналу даних, зібраних із шини CAN

Враховуючи те, що випробування проводилися на реальному транспортному засобі, необхідно було дотримуватись суворих часових вимог, щоб переконатися, що автомобіль не виявив помилок. Однією з головних проблем була заміна кадрів CAN FD, надісланих з комп’ютера, включаючи перетворення CRC, необхідного в механізмі наскрізного захисту. Логічний зв'язок представлений на рис. 3.16.

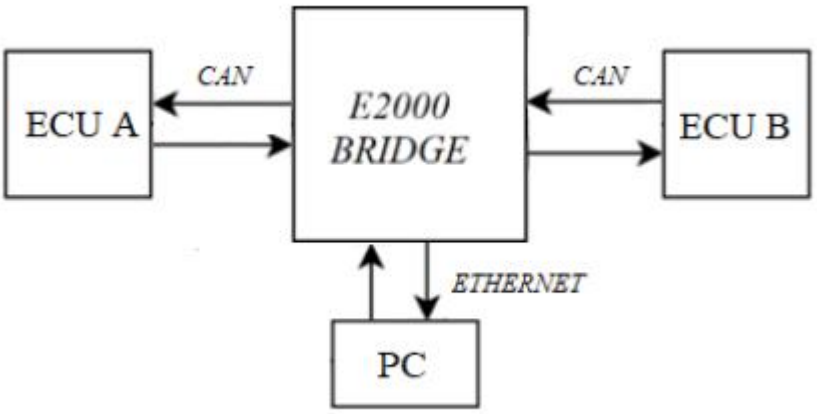


Рис.3.16. Схема детального логічного підключення пристрою MicroDAQ E2000

Тому для тестування було використано дуже швидкий пристрій MicroDAQ E2000 (рис. 3.17.). Пристрій відповідає всім вимогам часу, забезпечуючи прямий доступ до пам'яті через інтерфейс Ethernet. Слід підкреслити, що кадри, які замінювалися наступним чином, можна було відправляти паралельно на пристрій. Висновок, модуль MicroDAQ E2000, підключений у режимі мосту (пересилає кадри з одного боку шини на інший, і при необхідності може замінити вміст кадрів), був прозорим для тестованого автомобіля. Всі заміни рам не викликали постійних збоїв в роботі автомобіля при штатній експлуатації автомобіля.

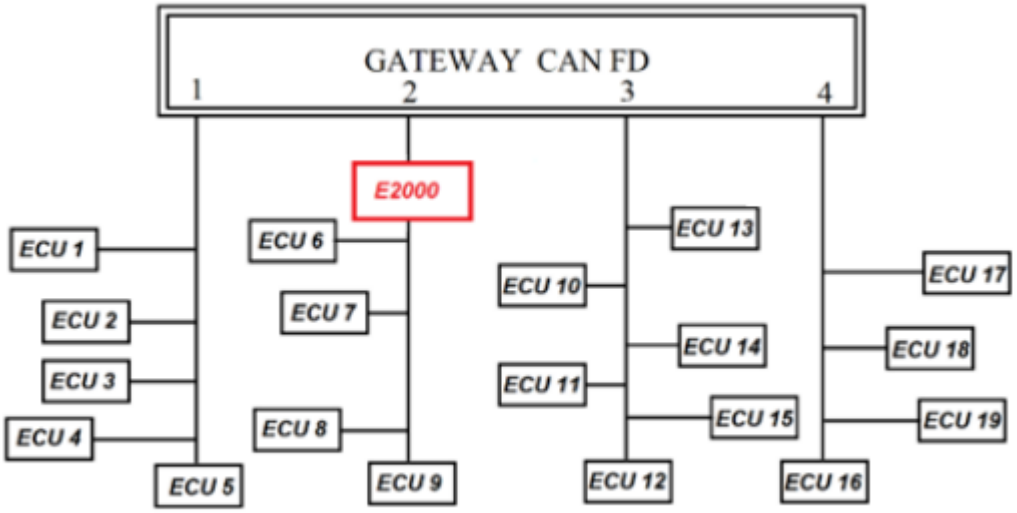


Рис.3.17. Схема системи, що тестується

Висновок до 3 розділу

У даному розділі були розглянуті вибрані методи, що дозволяють знайти сигнали, що керують певною функціональністю автомобіля. Процедура завжди починається з концепції реєстрації керуючої інформації з шини CAN, коли покажчик повороту вимкнено. Наступним кроком є коригування зібраних даних і підготовка списку рамок CAN для заміни, коли покажчик повороту активний. Було доведено, що можна знайти послідовність бітів, що керують заданою функціональністю. Очікуваним результатом було знайти рамку або кілька рамок CAN, які збираються вимкнути покажчик повороту, коли він був увімкнений, після заміни. Для заміни вмісту кадрів, коли в кадрі присутній механізм наскрізного захисту, використовувався метод зворотного проектування, а всі необхідні ключові значення були знайдені методом підбору. На наступному етапі експерименту, вже звузивши перелік ідентифікаторів кадрів, які могли б відповідати за управління покажчиком повороту, був використаний інший метод.

РОЗДІЛ 4. РОЗРОБКА ТА ВИЯВЛЕННЯ КІБЕРАТАКИ НА РУЛЬОВИЙ МЕХАНІЗМ

4.1. Виявлення кібератаки на рульовий механізм за допомогою підходу на основі штучного інтелекту

Основною метою дослідження, проведеного в рамках цього експерименту, було довести, що за допомогою обраних алгоритмів штучного інтелекту можна виявити триваючу атаку на електронний модуль управління в електромобілі.

Було зроблено припущення, що під час нападу на транспортний засіб сигнали, які надсилаються через CAN-шину у вигляді байтів даних покажуть аномальну картину, тобто буде виявлено стан, відмінний від очікуваного під час звичайної роботи [16-17]. Експеримент проводився без доступу до документації досліджуваного автомобіля, тобто без знання сигналів керування автомобілем. З огляду на це використовувався підхід "чорного ящика".

Дані, що реєструються з CAN-шини, розглядалися як послідовність байтів, серед яких повинні бути і керуючі сигнали. Підхід, що розроблявся в ході дослідження, базувався на виявленні аномалій за допомогою глибокої нейронної мережі. На основі мережі можна було проаналізувати дані, що з'являються на CAN-шині, та врахувати часові залежності між ними. Найважливішим аспектом є можливість визначення моменту атаки. Елемент автомобіля, на який була здійснена атака, позначений на рис. 4.1 і відповідає рульовому управлінню.

Рис.4.1. Рульове управління

Дослідження, проведені під час експерименту, були поділені на етапи, які характеризуються нижче. Об'єктом атаки був модуль управління рульовим керуванням електромобіля. Можливість перехоплення контролю над операцією повороту слід розглядати як найбільш серйозну загрозу, оскільки це може призвести до аварії, тобто серйозною загрозою, оскільки це може легко призвести до аварії, тобто загрози здоров'ю та життю учасників руху здоров'ю та життю учасників дорожнього руху.

Передбачалося, що виявлення атаки можливе шляхом виявлення аномалій в керуючих даних, що містяться в переданих CAN-кадрах. Таким чином, необхідно було реєструвати значення сигналів, а фактично окремі байти в полях даних переданих кадрів. Це здійснювалося як під час звичайної експлуатації автомобіля, так і під час атаки. Крім того, сценарій так званої звичайної експлуатації було розширено за рахунок додаткових даних, що реєструються при використанні системи допомоги водієві, яка називається LANE_ASSIST_MODE. Було проведено десятки випробувань і понад 20 годин тестів на реальному електромобілі. Значення даних, що з'являються на CAN-шині, збиралися і зберігалися у файлах у 3 типах ситуацій, представлених на рис. 4.2. 17]:

- звичайний режим руху (водій керує транспортним засобом без увімкненої системи допомоги при утриманні в смузі руху) - REGULAR_MODE;
- рух з увімкненою системою допомоги при утриманні в смузі руху - LANE_ASSIST_MODE;
- рух, коли було здійснено успішний напад, і управління рульовим керуванням було керування автомобілем - ATTACK_MODE.

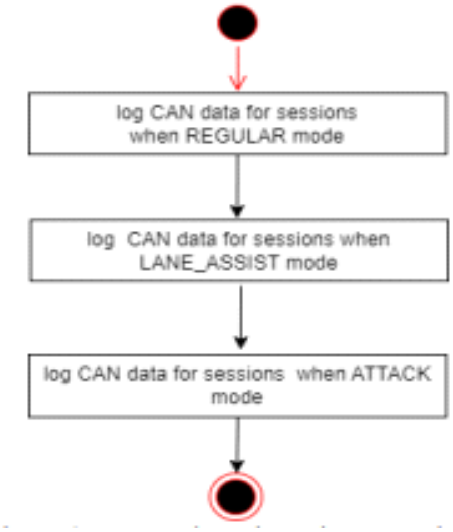


Рис.4.2. Сеанси реєстрації даних CAN

Відповідно до концепції "чорного ящика" і через відсутність доступу до документації, що містить сигнали управління тестованого автомобіля, необхідно було припустити, що серед даних є сигнали рульового механізму, що відповідає за управління.

Зібравши кілька гігабайт даних у вигляді кількох десятків сеансів, необхідно було перетворити їх у формат, який би дозволив подальшу обробку даних. В основі концепції лежить карта байт, розташованих у часі з роздільною здатністю 1 мілісекунда. Наступні байти завжди згруповані відповідно до CAN ідентифікатора в одному і тому ж порядку, як показано на рис. 4.3.

Байти з полів даних вибраних CAN-кадрів були з'єднані разом у такому порядку: 0x40 (довжина = 8) + 0x86 (довжина = 8) + 0xFD (довжина = 8) + 0x116 (довжина =8) + 0x176 (довжина = 8) + 0x31B (довжина = 8) + 0x65D (довжина = 8) + 0x303 (довжина = 24) + 0xFC (довжина = 48) + 0x102 (довжина = 48).

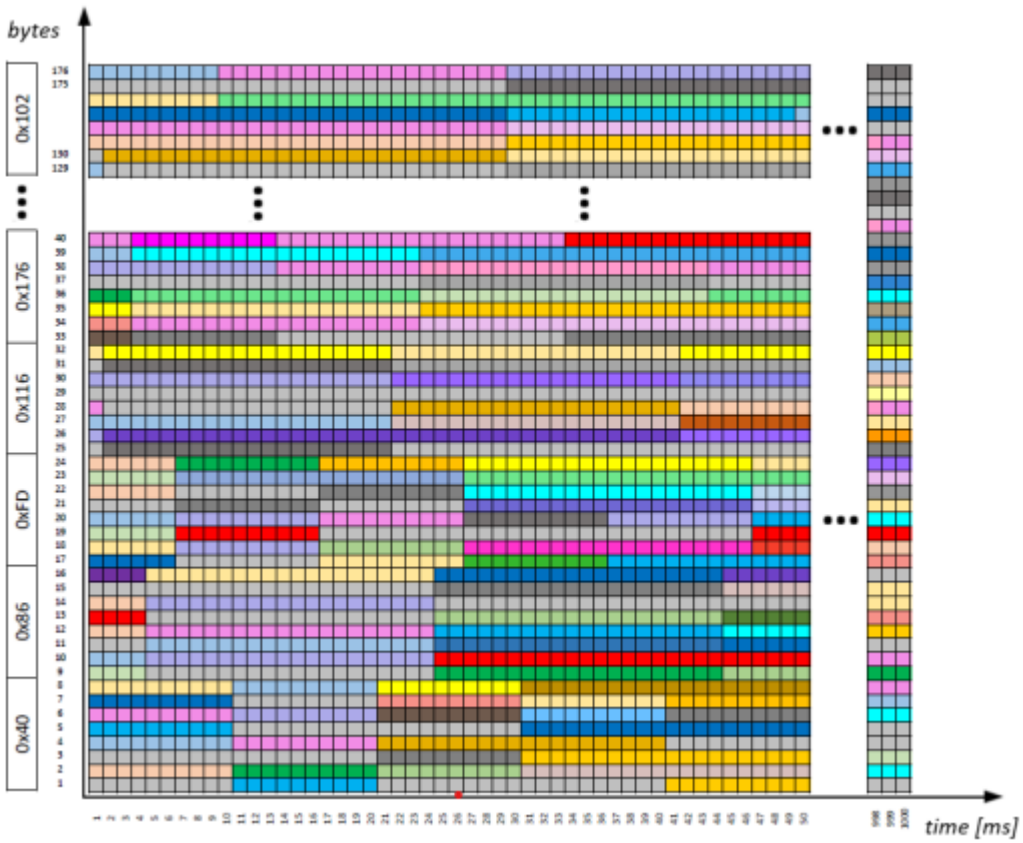


Рис.4.3. Концепція байтової карти з призначеним представленням байтів кольору на один раз

Відповідно до стандарту протоколу CAN, кадри надсилаються на шину циклічно з певним часом циклу. Значення часу циклу задається в мілісекундах і його величина залежить від важливості функції, яку виконують сигнали, що входять до складу одного кадру. Чим вищий пріоритет інформації, що передається, тим менше значення часу циклу. Типові значення тривалості циклу коливаються від десяти до кількох тисяч мілісекунд.

Для отримання часової роздільної здатності в 1 мілісекунду зібрані дані оброблялися за допомогою скриптів Python таким чином, щоб байти даних для наступних мілісекунд дублювалися з даними, отриманими в останньому CAN-кадрі. Крім того, дані були підготовлені таким чином, що дані з усіх CAN-кадрів для кожного ідентифікатора зберігалися в окремому файлі, при цьому забезпечувалася консистентність даних, тобто їх синхронізація в часі.

Крім того, був встановлений фіксований часовий інтервал для тривалості одного сеансу близько 5 хвилин. Концепція підготовки даних, отриманих в результаті процесів входу в систему, детально представлена на рис. 4.4.

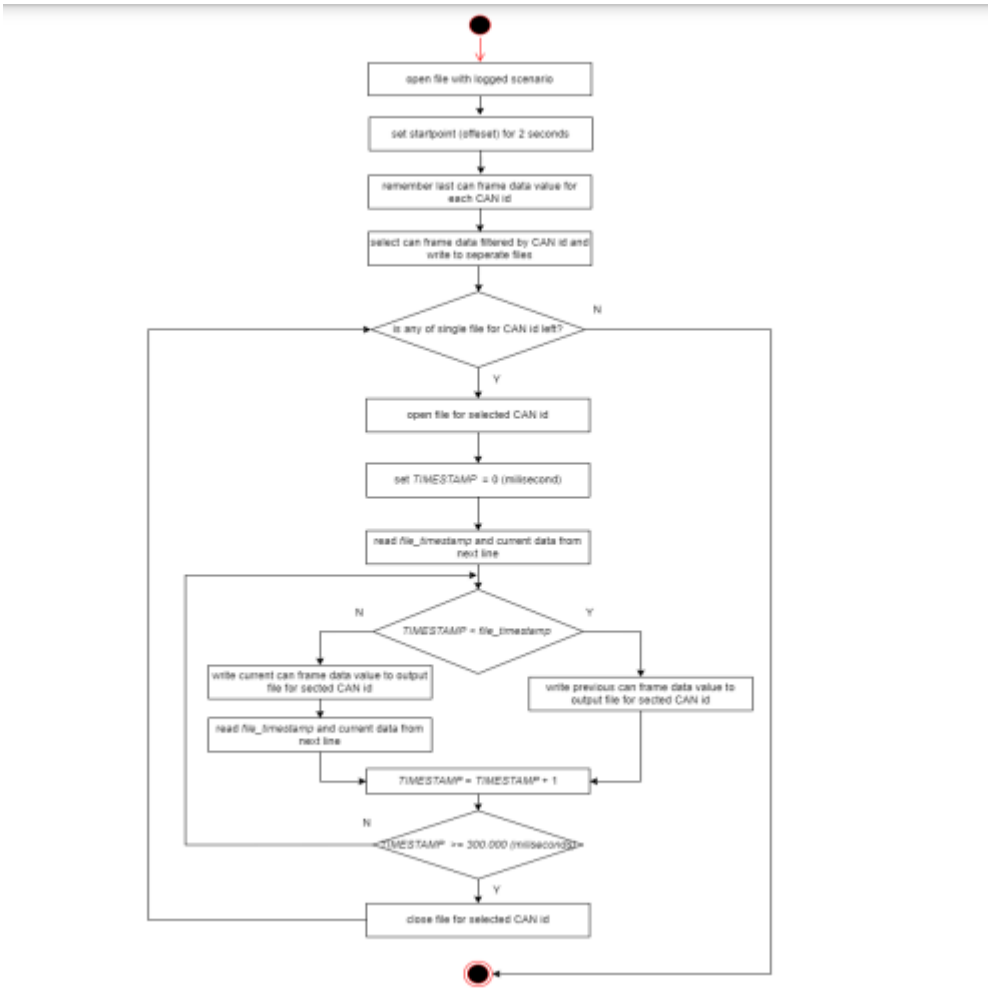


Рис.4.4. Схема концепції підготовки окремих файлів для кожного CAN ідентифікатора з роздільною здатністю 1 мілісекунда

Наступним етапом експерименту було використання підходу штучного інтелекту для пошуку аномалій. Це було зроблено після того, як CAN-повідомлення були записані та оброблені за допомогою скриптів на мові Python. Теоретично, маючи дані, записані під час звичайної експлуатації автомобіля, можна навчити нейронну мережу і виявити момент виникнення аномалії, що розуміється як ознака триваючої атаки на транспортний засіб.

Для цього були використані алгоритми глибокого навчання, що враховують часові залежності між оброблюваними даними. Тести виявлення аномалій за допомогою мережі були проведені у 2 випадках:

- нейронна мережа навчалася на даних звичайного водіння. Електромобілем керував водій без увімкненого асистента руху по смузі. Детальний алгоритм представлений на рис. 4.5.

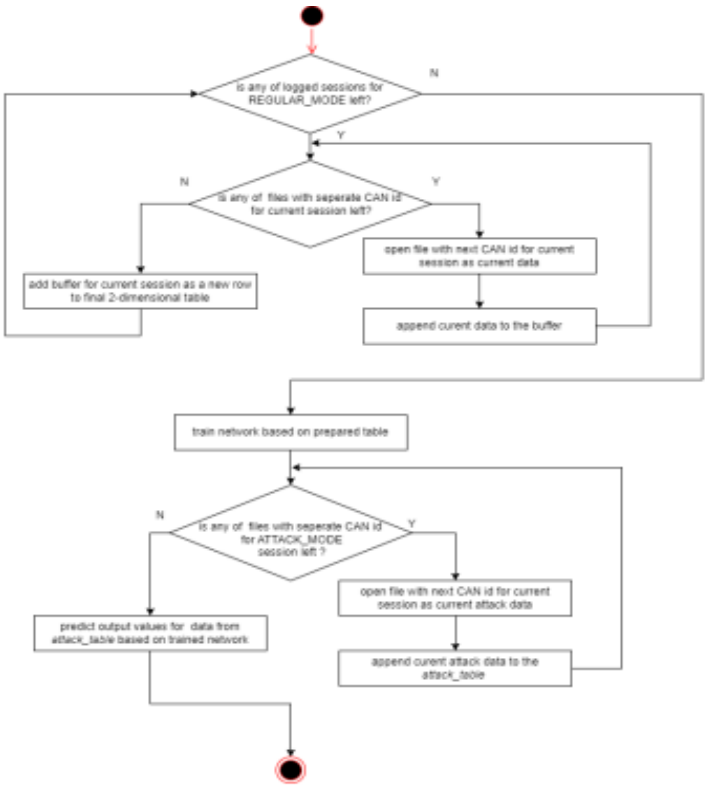


Рис.4.5. Детальна схема алгоритмів навчання для REGULAR_MODE

- нейронна мережа навчалася на даних звичайного водіння, коли електромобілем керував водій з увімкненим асистентом. Детальний алгоритм наведено на рис. 4.6.

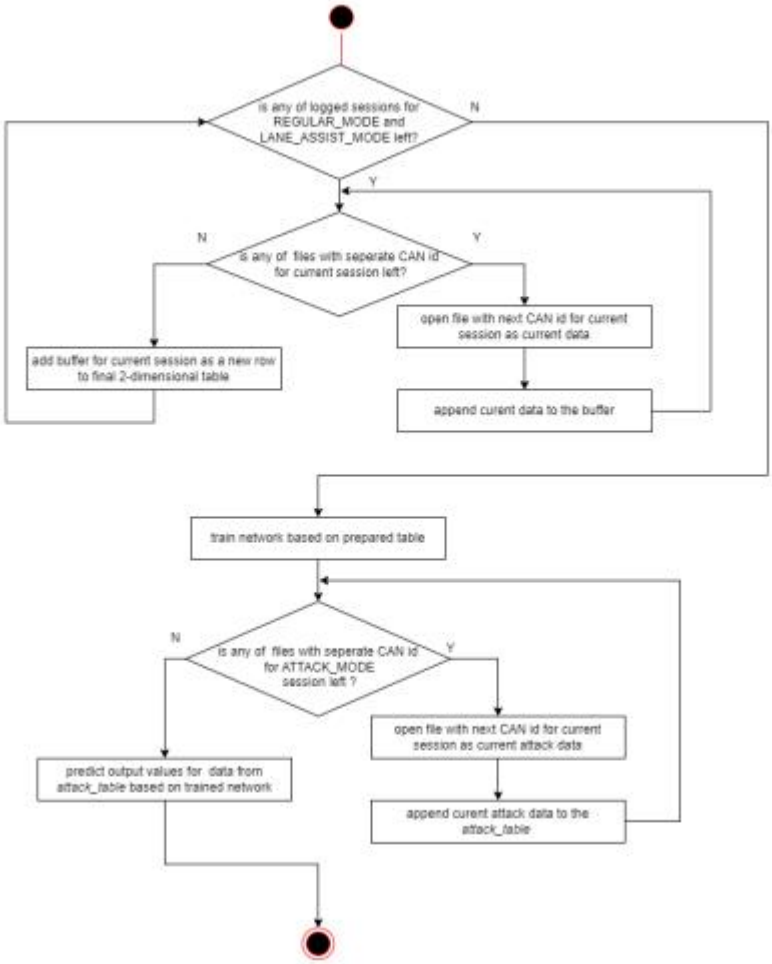


Рис.4.6. Детальна схема алгоритмів навчання для REGULAR_MODE та LANE_ASSIST_MODE

Для проведення експерименту були використані реальні дані, записані під час різних режимів експлуатації автомобіля для експерименту. Спочатку була проведена належна підготовка та налаштування як формату даних, так і синхронізації часу до запропонованої оригінальної концепції байтової карти.

Основна проблема, яка виникла, полягала у виборі методу аналізу даних, який може працювати у випадку такої великої кількості вхідних даних. Важливо зазначити, що дані залежать від часу. Основною метою цієї частини експериментів було виявлення атаки на основі ідентифікації аномалій, присутніх в даних. В експерименті було реалізовано метод з використанням автокодерів.

Враховуючи тип оброблюваних даних, той факт, що це дуже великі обсяги байтів, які циклічно надсилаються кожну мілісекунду, а також визначену довжину

поля даних у CAN-кадрах (для кожного ідентифікатора CAN-кадру), припускається, що існують певні шаблони даних, що повторюються. Це є основною причиною застосування методу глибокого нейронного навчання. Розрахунки проводилися з використанням спеціалізованого інженерного інструменту MATLAB з інструментарієм глибокого навчання.

В обраному алгоритмі було доступно 3 типи рекурсивних шарів для глибокого навчання з часовими рядами та послідовними даними:

- LSTM шар - довгий шар короткочасної пам'яті, вивчає довгострокові зв'язки між послідовними даними та часовими періодами
- шар BILSTM - двонаправлений довгий короткочасний шар пам'яті, шар LSTM
- вивчає двонаправлені довготривалі зв'язки між послідовними даними та часовими періодами
- Рівень GRU - gated recurrent unit layer, вивчає взаємозв'язок між послідовними даними та періодами часу.

Оскільки обсяг даних, що підлягають обробці, дуже великий (десятки гігабайт), а доступ до обчислювальних потужностей та доступ до обмежених обчислювальних потужностей, в експерименті було використано рівень GRU. Він працює швидше ніж модель з шаром LSTM завдяки своїй структурі.

Було припущено, що кількість вхідних одиниць у вхідному шарі дорівнює 168. Це випливає з кількості байт, які були включені в один рядок байтової карти.

Відповідно до принципу роботи автокодерної (неповної) мережі, наступний шар повинен містити зменшену кількість нейронів (оскільки відбувається процес кодування), тому другий шар GRU було обмежено до 84, що вдвічі менше, ніж у першого шару GRU. На останньому етапі, під час декодування, було створено повністю зв'язний шар з кількістю вхідних нейронів 168, тобто було досягнуто початкового розміру. Які саме шари використовувалися в моделі, показано на рис. 4.7.

```
% Define gru network layers
layers = [ sequenceInputLayer(featureDimension, 'Name', 'in')
   gruLayer(168,'Name', 'gru1')
   batchNormalizationLayer
   dropoutLayer(0.3)
   reluLayer('Name', 'relu1')
   gruLayer(84,'Name', 'gru2')
   batchNormalizationLayer
   dropoutLayer(0.3)
   reluLayer('Name', 'relu2')
   fullyConnectedLayer(featureDimension, 'Name', 'fc')
   regressionLayer('Name', 'out') ];
```

Рис.4.7. Шари, реалізовані в концепції автокодера

Тестова установка являла собою справжній електромобіль з невеликими змінами в з'єднаннях на центрального шлюзу для підключення додаткових пристроїв. Для зняття даних з CAN-шини, як і у випадку з іншими експериментами, використовувався стандартний пристрій PCAN-USB PRO, доступний на ринку.

Для виконання атак і взяття на себе управління та функції твістингу, тобто на практиці електронного модуля, що відповідає за управління рульовим керуванням, використовувався пристрій MicroDAQ E2000, що працює в режимі моста. Спосіб підключення до шлюзу представлено на рис. 4.8.

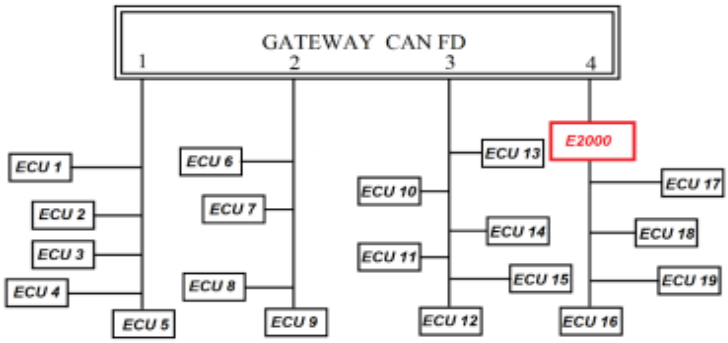


Рис.4.8. Схема тестованої системи з мостовим модулем, позначеним червоним кольором

Вимоги, яким мав відповідати тестовий пристрій Microdaq E2000, були дуже високими. Вони особливо важливі з точки зору часу, необхідного для обробки повного кадру CAN FD. Цей пристрій використовувався для атаки на модуль рульового управління шляхом заміни оригінального вмісту CAN-кадрів на кадри,

які були попередньо записані під час роботи системи допомоги при утриманні в смузі руху.

Завдяки цьому стало можливим взяти під контроль рульовим керуванням на реальному автомобілі. Проведені випробування не призвели до виявлення помилок автомобільною системою. Для атаки на систему управління використовується пристрій, що працює в режимі моста або пересилання інформації в CAN-кадрах від входу до виходу в обох напрямках. Це те, що показано на рис. 4.9.

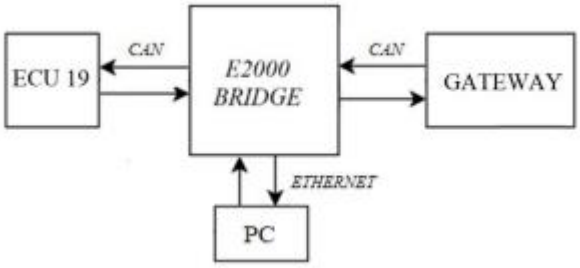


Рис.4.9. Детальна схема логічних з'єднань пристрою MicroDAQ E2000

Крім того, для конкретного CAN-кадру, що відповідає за скручування (ID=0x303), вміст поля даних було замінено на значення, надіслані через інтерфейс Ethernet з програми на персональному комп'ютері. Для керування кермом був використаний килимок (для комп'ютерних ігор), який був підключений до комп'ютера через Bluetooth. Повний набір пристроїв показано на рис. 4.10.

Рис.4.10. Набір пристроїв для контролю системи рульового керування: MicroDAQ E2000 як міст, блокнот, блокнот з додатком для ПК

Розроблене програмне забезпечення дозволило задавати бажані значення повороту з відповідним напрямком і моментом, зчитуючи поточне положення керма з пристрою Microdaq E2000. Це було представлено у графічному вигляді.

- Перевірочні тести

Зібравши дані з CAN-шини у випадках, коли автомобіль використовувався в так званому звичайному режимі, тобто автомобілем керує людина без увімкненого асистента утримання в смузі руху, та в режимі з увімкненим зібрані дані після обробки за допомогою Python-скриптів були реалізовані скрипти для навчання нейронної мережі. Запропонована модель байтової карти, тобто, наступні байти полів даних CAN-кадрів розташовуються завжди в одному і тому ж порядку. Вони навчаються за допомогою мережі типу GRU-AE. Це навчання було розділене на 2 етапи.

На першому етапі використовувалися дані, зібрані під час звичайного руху, тобто без увімкненого асистента руху по смузі. Важливим фактором, який змушував кермо рухатися, був навмисний маневр водія. Як видно на рис. 4.11., можна було помітити аномалію, яка виникла під час триваючої атаки, тобто взяття під контроль функції повороту автомобіля.

Однак, отримана різниця між сигналом, що свідчить про виникнення аномалії та сигналом на виході мережі для коректного випадку не є суттєвою. Можна зробити висновок, що необхідно використовувати більше навчальних даних під час навчання для отримання більшого значення залишків.

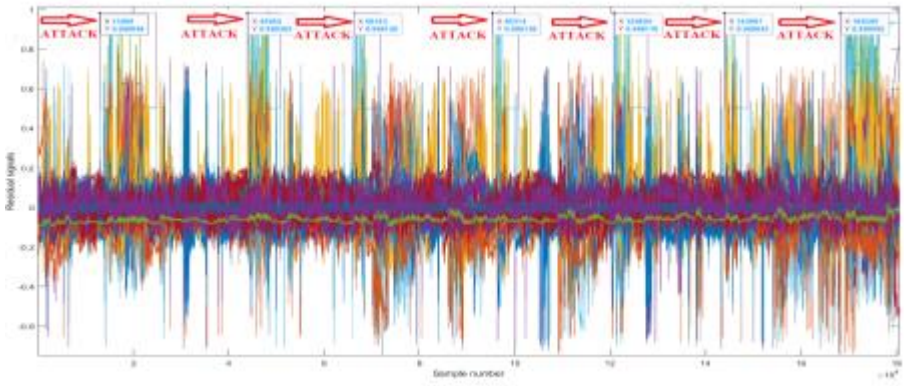


Рис.4.11. Виявлення аномалії (атаки) за допомогою DNN GRU-AE, навченого без допомоги смуги руху

На другому етапі дослідження використовували дані, зібрані під час руху, коли за поворот відповідали обидва водій і система асистента керування смугою руху відповідали за розворот автомобіля. Як видно на рис. 4.12., вдалося помітити аномалію, яка виникла під час триваючої атаки, тобто перехоплення контролю над функцією повороту автомобіля.

Отримана різниця між сигналом, що свідчить про виникнення аномалії, і сигналом на виході мережі для правильного випадку були настільки значними, що можна було легко відрізнити правильний сигнал від аномалії, або точно і без сумнівів вказати момент атаки.

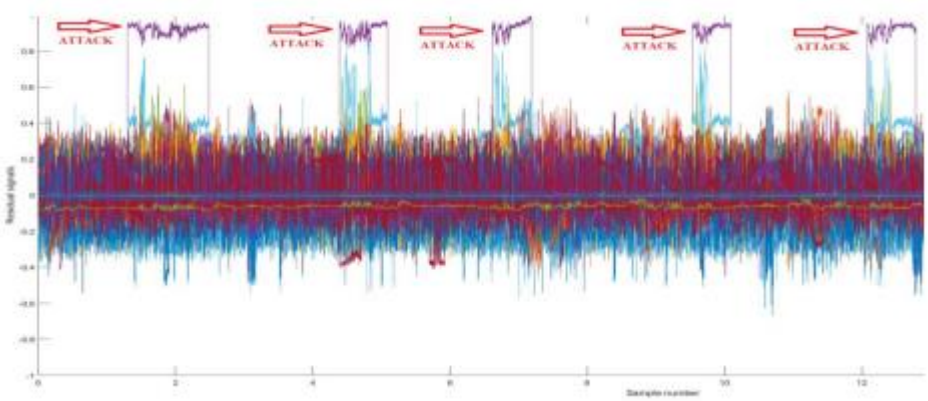


Рис.4.12. Виявлення аномалії (атаки) за допомогою DNN GRU-AE, навченого з підтримкою смуги руху

Тут варто підкреслити, що експеримент довів, що можна успішно атакувати сучасний електромобіль і взяти його під свій контроль. У разі отримання контролю над такими ключовими системами управління, як гальмування, прискорення або поворот, описаними в цій частині роботи.

Оскільки атаки такого типу є дуже небезпечними, тому так важливо продовжувати дослідження, спрямовані на підвищення безпеки в автомобілях.

Розглядаючи результати попередніх експериментів, чітко видно, що застосування методів, заснованих на штучному інтелекті, а особливо навчання, значно підвищує можливість виявлення атак.

4.2. Зведення дослідів і перевірочних випробувань. Запропоновані підходи до захисту автомобіля

Для виявлення атаки було використано автокодер глибоких нейронних мереж, що використовує ГРУ як інструмент виявлення аномалій. Порівняння між стисненням вихідних даних, а декомпресією вихідних даних з урахуванням часових залежностей показало, що виявити атаку можна [18].

Також було доведено, що виявити атаку можна, вивчивши глибоку нейронну мережу на даних, зібраних під час звичайного водіння без активної системи допомоги при утриманні в смузі руху. Однак різниця між очікуваним значенням на виході мережі та аномалією виявилася несуттєвою. Слід також підкреслити, що якщо мережа додатково навчалася на даних, зібраних під час руху з увімкненою активною системою утримання в смузі руху, то різниця була суттєвою.

Експеримент довів, що завдяки використанню глибоких нейронних мереж можна зі 100% ефективністю виявляти атаки і таким чином готувати відповідний сценарій на рівні транспортного засобу, який зможе запобігти подібним ситуаціям або принаймні мінімізувати їхні наслідки.

В автомобільній промисловості, де обсяг виробництва обчислюється мільйонами штук, особливий акцент робиться на мінімально можливу вартість виробництва одного модуля. Тому, незважаючи на те, що існують ефективні методи шифрування з використанням спеціального апаратного забезпечення, вони зазвичай не реалізуються в системах, які контролюють критичні функції транспортних засобів. Впровадження таких методів і пристроїв підвищує вартість автомобіля. Саме тому в більшості випадків дані про автобуси передаються відкрито, створюючи ризик неналежного використання. Враховуючи очікування щодо зниження витрат і забезпечення безпеки автомобіля, потрібно використовувати прості методи шифрування. Такі підходи були розроблені в рамках PhD проекту і представлені нижче. Вони є результатами експериментів, описаних у попередньому розділі дипломної роботи.

1. Концепція часового вікна

Концепція передбачає додавання деякої інформації в поле даних кадру CAN. Він відомий як мітка часу, яка перевіряє дійсність переданих даних. В якості мітки часу використовується поточне значення часу, відраховане від початку всієї системи. Його початкове значення визначається спеціальним CAN-кадром, який при запуску системи передається через пристрій, що керує іншими модулями. Потім він синхронізується кожний вказаний час (наприклад, 10 секунд). За замовчуванням мітка часу використовує 1 байт (це означає, що в одному кадрі CAN можна надіслати меншу кількість даних), але її можна легко розширити до 2 байтів. Перевірочні випробування довели ефективність цього методу. Було зазначено, що 100% ефективності отримати неможливо. Однак метод істотно мінімізує ймовірність успішної атаки. Чим коротше вікно часу і більше число бітів, виділених для лічильника часу життя, тим вище ефективність описаного методу. Припускаючи наступне:

• 16 біт використовується для лічильника часу життя

• значення часового вікна встановлено на 100 мілісекунд

• надсилання кадрів CAN можливе з роздільною здатністю 1 мілісекунда.

Імовірність проведення успішної атаки повтору кадрів наближається до 0%.

$$P_{SA} = \frac{1}{65536} * \frac{100ms}{1ms} = 0{,}15\% \tag{4.1}$$

P_{SA} – ймовірність успішної атаки, що означає ефективність захисту 99,85%.

2. Концепція XOR

Основою цієї концепції є посилання на те, як працює логічна функція XOR (виключне АБО). Якщо значення байта двічі виконується XOR з тим самим аргументом, результат обмежується початковим значенням. Іншими словами, відправник кадру виконує ключову операцію byte[x] XOR (де x — індекс поля даних із CAN-кадру). В результаті виходить зашифрована інформація. Одержувач виконує ту саму операцію з ключем байт[x] XOR і таким чином отримує вихідне значення даних. Однак під час передачі вони просто шифруються.

3. Концепція заперечення подвійних бітів

Концепція є розширеною версією «концепції вікна часу». Підхід заснований на подвійному запереченні бітів у кожному байті переданого кадру, для якого відповідні біти значення аргументу цієї операції дорівнюють 1. Іншими словами, для бітів, які відповідають значенню 1 в аргументі виконується порозрядне заперечення, а решта бітів не змінюється. Операція проводиться двічі. На першому кроці значення операнда є ключем, а на другому кроці значення операнда пов’язане з вікном часу. 8-бітне значення ключа зберігається в енергонезалежній пам'яті кожного ECU, підключеного до шини CAN. Одержувач кадру виконує зворотний процес, тобто спочатку скасовує, використовуючи значення часового вікна як аргумент, а потім ключ, що зберігається в енергонезалежній пам’яті. В таблиці 4.1 показані наступні кроки запропонованого елементарного алгоритму шифрування.

Таблиця 4.1. Приклад застосування запропонованого шифрування

Значення	Шістнадцяткове значення	Двійкова величина
оригінальний байт	0x7D	01111101
ключ (маска для заперечення)	0xC3	11000011
зашифрований байт – крок 1	0xBE	10111110
часове вікно	0xF1	11110001
останній зашифрований байт	0x4F	01001111

4.2.1. Концепція модуля захисту від злому шини CAN, що підтримується алгоритмами на основі штучного інтелекту

Запропонована концепція є компромісом між збереженням низької вартості виробництва модулів та ефективним виявленням атаки. За допомогою розробленого рішення можна відреагувати та уникнути втрати контролю над деякими модулями транспортного засобу. Слід підкреслити, що удосконалення існуючої архітектури передачі даних на основі CAN-шини з використанням додаткового модуля супервізора додатковим модулем-супервайзером вимагає додаткових витрат через велику кількість CAN інтерфейсів та високої обчислювальної потужності.

Навіть така важлива функція, як рульове управління, яке має бути особливо захищеним. Оскільки ефективна атака на електронний виконавчий модуль

можливий, і в той же час вартість автомобіля не може суттєво підвищити, було запропоновано модуль захисту від злому CAN-шини. Підхід використовує алгоритми штучного інтелекту для виявлення аномалій під час аналізу трафіку шини CAN трафіку CAN-шини. Основне припущення підходу полягає в тому, що кожна виявлена аномалія може вказувати на триваючу атаку. Однак це все ще є найкращим рішенням, враховуючи, що кількість електронних блоків керування в сучасному автомобілі становить від 100 до 200[19]. Архітектура розробленої концепції представлена на рис. 4.13.

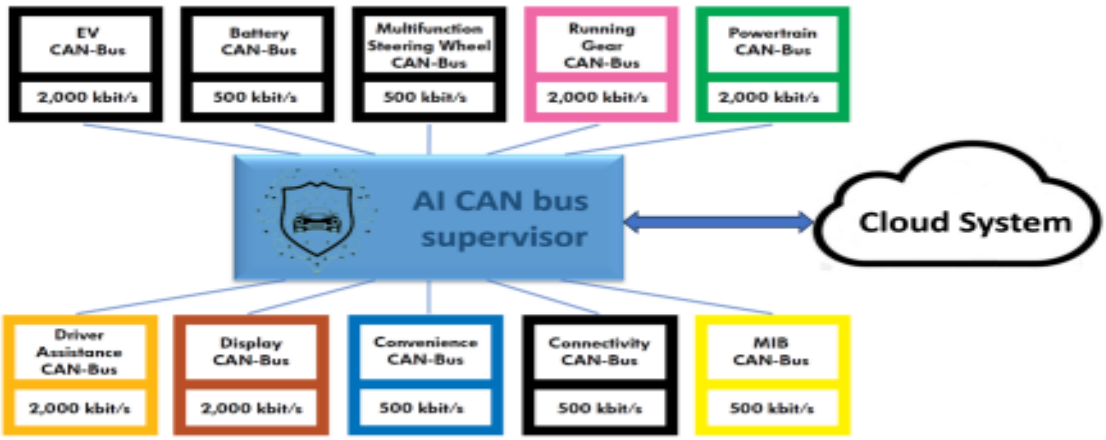


Рис.4.13 Концепція модуля захисту від злому шини CAN відповідно до ідеї Індустрії 4.0

Найбільша проблема виникла в процесі навчання нейронної мережі.

Незважаючи на високу обчислювальну потужність і виділену відеокарту з незалежною оперативною пам'яттю об'ємом 24 ГБ, для навчання мережі знадобилося понад 20 годин. Оскільки супервізорний модуль, який би міг навчатися "на льоту" за певний час і підтримувати кілька десятків інтерфейсів CAN-шини, такий підхід виявився занадто дорогим.

Враховуючи сучасний стан розвитку інформаційних технологій, можна скористатися підходами, пов'язаними з "Індустрією 4.0". В результаті всі розрахунки та операції, які потребують багатодоступних ресурсів, виконуються в хмарі. Архітектура такої системи показана на рис. 4.14.

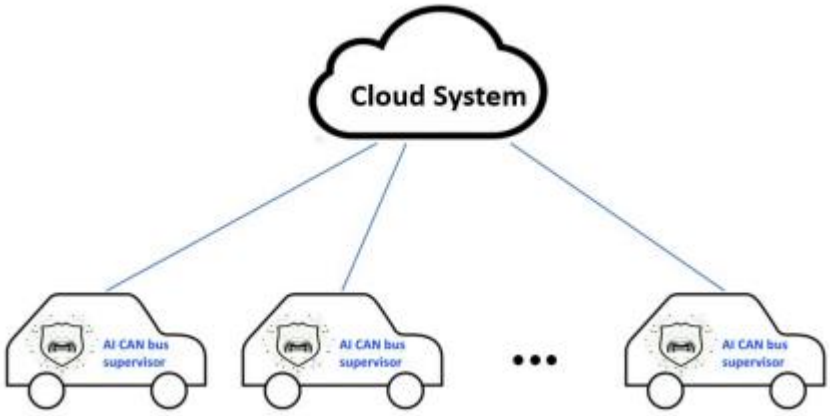


Рис.4.14. Концепція автомобілів, підключених до хмарної системи відповідно до екосистеми Індустрії 4.0

Модуль, встановлений у кожному транспортному засобі, надсилає попередньо оброблені дані до хмарної системи, де відбувається процес навчання. Необхідність попередньої обробки даних зумовлена через їх початковий великий розмір. Такий підхід має кілька переваг. Найважливіша з них полягає в тому, що всі транспортні засоби оснащені найновішою моделлю зібраних даних отриманих на основі всіх активних транспортних засобів. Досить, щоб один транспортний засіб був атакований невідомим до цього часу досі невідомим методом, а завдяки хмарному навчанню та розповсюдженню навченої моделі на контрольні модулі в автомобілях, кожен автомобіль є стійким до цього нового типу атак.

Це дає можливість бути стійким до досі невідомого типу загрози. Таким чином, представлений концепт є інтелектуальною самонавчальною моделлю, яка здатна ефективно виявляти невідомі типи загроз.

Висновок до 4 розділу

Було виконано заплановану послідовність дій, спрямованих на виявлення аномалій. Передбачалося, що виявлення аномалії може становити інформацію про атаку на машину. Дані реєструвалися з CAN-шини, безпосередньо з'єднаної з системою рульового керування. Експерименти проводилися під час руху у звичайному режимі та з активною системою допомоги при утриманні в смузі руху. Крім того, дані з CAN шини знімалися під час атаки, яка полягала в перехопленні контролю над функцією повороту автомобілю. Для цього було проведено реальний сценарій кібератаки з використанням додаткового пристрою Microdaq

E2000, що працює в режимі моста і керується з комп'ютера додаток через шину Ethernet. Доведено, що можна успішно атакувати сучасний електромобіль і отримати контроль над ним непомітно для системи керування транспортним засобом.

ВИСНОВКИ

Сучасний автомобіль розуміється як інтелектуальний мехатронний транспортний засіб, інтегрований із системою управління, що відповідає різним аспектам концепції «Індустрії 4.0». У ході дослідження було доведено, що в сучасному електромобілі можна керувати наступними модулями управління в транспортному засобі: внутрішнім освітленням, поворотником і функцією рульового управління. Також було опрацьовано наступні завдання:

1. Описано процес проектування сучасного автомобіля. Опис базується на порівнянні з минулими підходами. Визначено напрямки розвитку автомобільних систем, які трансформувалися від механічних до мехатронних. У розділі перераховані потенційні небезпеки для систем автомобіля, як незахищені прогалини для кібератак. На основі проаналізованої літератури перераховано можливі типи кібератак, а також охарактеризовано приклади успішно проведених атак на автомобілі. Крім того, у цьому розділі розглядається література, щоб дослідити поточні заходи безпеки, що застосовуються в автомобілях.
2. Описано багатофункціональний пристрій збору даних MicroDAQ E2000 із можливостями обробки в реальному часі, розглянуто його особливості, специфікацію та підтримувані операційні системи. Також PCAN-USB Pro Інтерфейс CAN і LIN для високошвидкісного USB 2.0, наведені його особливості, властивості роботи та його призначення.
3. Вибрано методи, що дозволяють знайти сигнали, що керують певною функціональністю автомобіля. Процедура завжди починається з концепції реєстрації керуючої інформації з шини CAN, коли покажчик повороту вимкнено. Наступним кроком є коригування зібраних даних і підготовка списку рамок CAN для заміни, коли покажчик повороту активний. Було доведено, що можна знайти послідовність бітів, що керують заданою функціональністю. Очікуваним результатом було знайти рамку або кілька рамок CAN, які збираються вимкнути покажчик повороту, коли він був увімкнений, після заміни. Для заміни вмісту

кадрів, коли в кадрі присутній механізм наскрізного захисту, використовувався метод зворотного проектування, а всі необхідні ключові значення були знайдені методом підбору. На наступному етапі експерименту, вже звузивши перелік ідентифікаторів кадрів, які могли б відповідати за управління покажчиком повороту, був використаний інший метод.

4. Виконано заплановану послідовність дій, спрямованих на виявлення аномалій. Передбачалося, що виявлення аномалії може становити інформацію про атаку на машину. Дані реєструвалися з CAN-шини, безпосередньо з'єднаної з системою рульового керування. Експерименти проводилися під час руху у звичайному режимі та з активною системою допомоги при утриманні в смузі руху. Крім того, дані з шини CAN шини знімалися під час атаки, яка полягала в перехопленні контролю над функцією повороту автомобілю. Для цього було проведено реальний сценарій кібератаки з використанням додаткового пристрою Microdaq E2000, що працює в режимі моста і керується з комп'ютера додаток через шину Ethernet. Доведено, що можна успішно атакувати сучасний електромобіль і отримати контроль над ним непомітно для системи керування транспортним засобом.

Завдяки новим технологіям, а також вимогам користувачів та їх безпеці обслуговування мехатронних систем є великим викликом. Складність полягає в тому, що при регулярній безпечній роботі таких систем необхідно забезпечувати діагностику на вимогу в режимі реального часу. Такі підходи, що працюють в режимі реального часу, є додатковими записами потенційних атак. Запропоновані концепції модулів кібербезпеки є відповідями на ці типи загроз. Ідея його роботи, викладена в дипломній роботі, базується на безперервному аналізі реальних правильних сигналів (тобто коли передбачалося, що атака не відбувається). Один із підходів базується на застосуванні алгоритмів штучного інтелекту, зокрема реалізовано нейронні мережі. Вирішальним аспектом у цьому випадку є постійний моніторинг передачі, а метою є виявлення аномалій, які розуміються як потенційна

можливість поточної атаки. Очевидно, що залежно від використовуваних технологій і шин комунікаційні інтерфейси повинні бути адаптовані. Однією з найбільших переваг представленого підходу є те, що можна реалізувати безперервний процес самонавчання.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Advanced Driver Assistance Systems (ADAS). (2023). Retrieved 08 23, 2023, from https://www.chipsaway.biz/blog/advanced-driver-assistance-systems-adas
2. Aliwa, E., Rana, O., Perera, C., & Burnap, P. (2021). Cyberattacks and countermeasures for in-vehicle networks. ACM Computing Surveys (CSUR), 1-37.
3. Andrade, R., Santos, M., Justo, J., Yoshioka, L., Hof, H.-J., & Kleinschmidt, J. (2023). Security architecture for automotive communication networks with CAN FD. Retrieved from https://www.sciencedirect.com/science/article/pii/S016740482300113X
4. Aries, K. (2021, 6 4). What Is V2V Technology?: V2V vs V2I vs V2X Technology Systems. Retrieved 08 02, 2023, from https://www.verizonconnect.com/resources/article/connected-vehicletechnology-v2v-v2i-v2x/
5. Asfa, I. (2023). Parts of a car and their functions explained. Retrieved 08 28, 2023, from https://engineerine.com/parts-of-a-car/
6. Autoencoders. (2023). Retrieved from https://www.mathworks.com/discovery/autoencoder.html
7. Babaghayou, M., Labraoui, N., Ari, A., Ferrag, M., & Maglaras, L. (2020). The Impact of the Adversary's Eavesdropping Stations on the Location Privacy Level in Internet of Vehicles. 2020 5th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDACECNSM), (pp. 1-6). doi:10.1109/SEEDA-CECNSM49515.2020.9221839.
8. Bosch, R. (1991). Specification version 2.0. Published by Robert Bosch GmbH (September 1991). Retrieved 08 28, 2023, from http://esd.cs.ucr.edu/webres/can20.pdf
9. Buttigieg, R., Farrugia, M., & Meli, C. (2017). Security issues in controller area networks in automobiles. 2017 18th International Conference on Sciences and

Techniques of Automatic Control and Computer Engineering (STA), (pp. 93-98). doi:10.1109/STA.2017.8314877

10. Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H., Savage, S., . . . Kohno, T. (2011). Comprehensive experimental analyses of automotive attack surfaces. 20th USENIX security symposium (USENIX Security 11), (pp. 77-92).
11. Choi, J., & Jin, S.-i. (2019). Security Threats in Connected Car Environment and Proposal of In-Vehicle Infotainment-Based Access Control Mechanism. Advanced Multimedia and Ubiquitous Engineering, (pp. 383–388).
12. D'Andrada, L., Araujo-Filho, P., & Campelo, D. (2020). A Real-time Anomaly-based Intrusion Detection System for Automotive Controller Area Networks. Brazilian Symposium on Computer Networks and Distributed Systems. Retrieved from https://api.semanticscholar.org/CorpusID:234531030
13. Das, S., Bhowmik, S., & Giri, C. (2017). Design of asynchronous semantic preamble listening for semantic sensor network to avoid early overhearing. 2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), (pp. 420-424). doi:10.1109/WiSPNET.2017.8299790
14. Desnitsky, V., & Kotenko, I. (2014). Expert Knowledge Based Design and Verification of Secure Systems with Embedded Devices. Availability, Reliability, and Security in Information Systems (pp. 194–210). Springer International Publishing.
15. Fahami, H., Zamzuri, H., Mazlan, S., & Zulkarnain, N. (2013). The Design of Vehicle Active Front Steering Based on Steer by Wire System. Advanced Science Letters, 61-65. doi:10.1166/asl.2013.4706
16. Falch, M. (2022). CAN FD Explained - A Simple Intro [2023]. Retrieved from https://www.csselectronics.com/pages/can-fd-flexible-data-rate-intro
17. Forest, T., & Jochim, M. (2011). On the Fault Detection Capabilities of AUTOSAR's End-to-End Communication Protection CRC's. SAE Technical Papers. doi:10.4271/2011-01-0999
18. Gajdzik, M. (2023). Metodyka wykrywania i rozpoznawania sygnałów sterujących na magistralach CAN w nowoczesnych pojazdach samochodowych.

Materiały Konferencji Młodych Naukowców nt.: Analiza zagadnienia, analiza wyników - wystąpienie młodego naukowca - Edycja V, 28-29.01.2023, Kraków, (p. 43).

19. Gajdzik, M., Sternal, K., Timofiejczuk, A., & Przystałka, P. (2021). A Glimpse into the Low-Cost Protection Method Dedicated for Electric Cars. 2021 5th International Conference on Control and Fault-Tolerant Systems (SysTol). IEEE. doi:10.1109/SysTol52990.2021.9595347

ДОДАТОК

Які вбудовані системи є в автомобілі?

1. Антиблокувальна гальмівна система (ABS)

ABS запобігає блокуванню коліс під час гальмування. Це особливо корисно на слизькій поверхні. Основні компоненти АБС включають:

Електронний блок керування : ECU використовує дані з датчиків, щоб визначити, чи слід качати гальма.

Гідравлічний блок керування : Гідравлічний блок керування містить насоси, заповнені гідравлічною рідиною. Насоси подають тиск на гальмівні барабани, коли це необхідно.

Клапани : Гальма, розташовані в гальмівній магістралі, регулюють тиск, дозволяючи або блокуючи тиск, що прикладається до гальм.

Блок датчиків коліс : ці датчики перевіряють швидкість обертання коліс автомобіля.

Датчики прикріплені до коліс, щоб виявляти блокування або коли колесо припиняє рух і починає від'їжджати від землі.

По-перше, робочі етапи ABS передбачають натискання водієм педалі гальма. Потім датчики коліс виявляють занос або блокування, а згодом ABS запускає гальма.

ABS забезпечує контроль тяги, ритмічно відновлюючи зчеплення з колесами, які зісковзують із землею під час застосування гальм.
(ABS є попередником сучасних систем дротового керування, і ви знайдете більше про них нижче.)

2. Електронний контроль стійкості (ESC)

Система ESC підвищує стійкість автомобіля на дорозі. Він працює з антиблокувальною гальмівною системою (ABS), щоб уникнути ситуацій недостатньої або надмірної поворотності, які можуть спричинити занос.

Недостатня поворотність – це коли транспортний засіб втрачає зчеплення з передніми колесами і хоче штовхнути вперед носом вперед. Надмірна

поворотність - це коли задні колеса втрачають зчеплення з дорогою, і задня частина починає ковзати.

Ця система корисна, коли водій чомусь втрачає контроль над кермом. Він автоматично гальмує, щоб автомобіль рухався в заданому напрямку. Гальмування застосовується до різних коліс. Система працює з ABS, дозволяючи ESC сповільнювати обертання коліс.

У цій системі використовуються такі датчики:

- Датчик кута повороту керма
- Датчики обертів коліс
- Бічний датчик
- Датчик швидкості повороту

3. Система адаптивного круїз-контролю

Адаптивна система круїз-контролю контролює швидкість автомобіля, регулюючи положення дросельної заслінки. Він використовує датчики, щоб визначити швидкість і положення дросельної заслінки.

Ця система допомагає водієві безпечно їздити по дорозі в пробках. Наприклад, він дозволяє водієві рухатися на заданій швидкості, коли дорога вільна (круїз-контроль). Адаптивний означає, що автомобіль стежить за швидкістю транспортного засобу попереду та адаптує встановлену швидкість для відстеження транспортного засобу попереду.

4. Drive-by-Wire

Технологія Drive-by-wire замінює або доповнює традиційні механічні системи керування, які використовують гідравліку або кабелі, електронними системами керування. Ці системи використовують датчики та виконавчі механізми для керування елементами роботи автомобіля. Вони також можуть увімкнути нетрадиційні людино-машинні інтерфейси, такі як елементи керування, як-от джойстики чи пелюстки. Drive-by-Wire охоплює три центральні системи:

Steer-by-wire : відсутність фізичного зв’язку між кермом і шинами.

Електронне керування дросельною заслінкою : відсутність фізичного зв’язку між педаллю газу та дросельною заслінкою.

Гальмо по дроту : у фактичній електромеханічній версії цього немає гідравлічної частини, натомість датчики визначають, яка сила використовується. Рульове керування та гальмо за проводом (поки що) не так широко використовуються, але електронний контроль дросельної заслінки вже деякий час присутній у транспортних засобах. Низький рівень електронного керування дросельною заслінкою десятиліттями використовувався в автомобілях з комп'ютеризованим керуванням паливом.

На даний момент Tesla є одним із небагатьох автомобільних брендів на дорозі, які широко використовують усі типи систем керування дротами.

5. Блок керування подушками безпеки

Блок управління подушкою безпеки захищає передніх пасажирів від зіткнення головою в разі аварії.

Залежно від тяжкості аварії система активує відповідні системи безпеки. Датчики зіткнення надсилають інформацію до мікроконтролерів, щоб спрацювати подушки безпеки. Ці датчики визначають швидкість і швидкість обертання.

Блок керування подушками безпеки зберігає дані про аварії, які пояснюють події, що призвели до аварії.

Зібрані дані знадобляться під час розслідування причин ДТП. Наприклад, зібрана інформація може включати швидкість, з якою рухався автомобіль.

6. Телематична система

Телематика привносить в автомобіль кілька функцій. По-перше, він контролює бездротове відстеження та зв'язок з автомобілем і з нього.

Телематика дозволяє автомобілям спілкуватися з іншими пристроями через Інтернет. Автомобілі з вбудованими телематичними системами надсилають дані автомобіля виробнику для регулювання.

Записана інформація включає місцезнаходження автомобіля, тиск у шинах, рівень палива в баку та термін служби моторного масла. Цим керується виробник у створенні інструкцій з обслуговування.

7. Система датчиків дощу

Система датчиків дощу використовує інфрачервоне світло як основний сигнал для запуску склоочисників.

На передньому лобовому склі розміщений оптичний датчик, який випромінює інфрачервоне світло. Залежно від кількості відбитого світла оптичний датчик визначає швидкість роботи склоочисників.

8. Автомобільна система нічного бачення

Ця система забезпечує покращене нічне бачення для водія, щоб забезпечити кращу видимість вночі.

Створене світло виходить за межі досяжності фар. Система виявляє пішоходів або перешкоди поблизу дороги та виділяє будь-які небезпеки, які можуть бути небезпечними.

Пристрої нічного бачення (NVD), такі як інфрачервоні камери та радарні пристрої, підтримують системи нічного бачення. Ці пристрої працюють у режимах покращення зображення, тепловізору та активного освітлення. Ці системи відносяться до активних або пасивних категорій.

Динамічні системи використовують інфрачервоні джерела світла для освітлення на великій відстані попереду автомобільних фар. Rolls-Royce Motor Cars і Toyota є деякими брендами, які встановили ці системи у своїх автомобілях.

Пасивні системи працюють інакше. Вони використовують камери для фіксації теплового випромінювання, що випромінюється навколишніми предметами. Деякі марки автомобілів, які використовують системи пасивного нічного бачення, включають Cadillac, BMW і Audi.

9. Система клімат-контролю

Автомобілі повинні бути готові до будь-яких погодних умов. Підтримка комфортних умов у салоні є важливою для водія та пасажирів.

Вбудована в автомобіль система клімат-контролю регулює внутрішню температуру автомобіля. Підтримання належного мікроклімату в автомобілі впливає на безпеку автомобіля.

10. Система моніторингу сліпих зон

Система моніторингу сліпих зон допомагає підвищити безпеку, сповіщаючи водія. Часто транспортні засоби опиняються поза полем зору водія в бічних дзеркалах.

Ця система використовує радарні датчики, розташовані всередині лівої та правої сторін заднього бампера. Він використовує камери в бічних дзеркалах, щоб знаходити транспортні засоби в їхньому полі зору.

Сліпі зони частіше становлять проблему, коли водій намагається змінити смугу руху або припаркуватися.