

ПІДВИЩЕННЯ ЗАВАДОСТІЙКОСТІ ПЕРЕДАЧІ ДАНИХ ПО UART ПРИ НАЯВНОСТІ ЕЛЕКТРОМАГНІТНИХ ПЕРЕШКОД

Вінницький національний технічний університет

Анотація

У роботі досліджуються методи захисту послідовного інтерфейсу UART від електромагнітних перешкод у промислових умовах. Проаналізовано основні джерела електромагнітної інтерференції та їх вплив на надійність передачі даних. Розглянуто технічні рішення для підвищення завадостійкості: апаратні методи виявлення помилок (CRC), багатократне зчитування біта для фільтрації шумів, застосування диференціального інтерфейсу RS-485 та правильне екранування кабелів.

Ключові слова: UART, електромагнітні перешкоди, CRC, RS-485, промислова комунікація, завадостійкість.

Abstract

The paper investigates methods of protecting the UART serial interface from electromagnetic interference in industrial environments. The main sources of electromagnetic interference and their impact on data transmission reliability are analyzed. Technical solutions for improving noise immunity are considered: hardware error detection methods (CRC), multiple bit sampling for noise filtering, differential RS-485 interface implementation, and proper cable shielding.

Keywords: UART, electromagnetic interference, CRC, RS-485, industrial communication, noise immunity.

Вступ

Інтерфейс UART залишається одним з найпоширеніших способів послідовної передачі даних у вбудованих системах. Його популярність пояснюється простотою реалізації та надійною екосистемою промислового обладнання. Проте в реальних умовах експлуатації, особливо на виробництві та в промислових об'єктах, системи на базі UART постійно зазнають впливу різноманітних електромагнітних перешкод. Це призводить до втрати даних, спотворення інформації і навіть повних відмов комунікації [4, 6].

Останні дослідження показують, що електромагнітні перешкоди можуть не тільки випадково спотворювати сигнали, але й створювати можливості для цілеспрямованих атак на послідовну комунікацію. З кожним роком кількість електронного обладнання зростає, а разом з ним зростає і рівень електромагнітного забруднення. Тому питання надійності передачі даних стає все більш критичним для промислових систем [11].

Джерела електромагнітних перешкод та методи виявлення помилок

Проблеми з UART комунікацією виникають через різні типи електромагнітних перешкод. Найчастіше це зовнішні перешкоди від електричного та механічного обладнання, яке працює поруч і створює електромагнітний шум. Також суттєвий вплив мають перехресні перешкоди від інших каналів комунікації, які розташовані на одній платі чи в одному кабельному джгуті. Окрему небезпеку становлять перешкоди від мережі живлення на частоті 50 -60 Гц, які через індуктивний зв'язок потрапляють у сигнальні лінії. Радіочастотні джерела теж можуть наводити перешкоди, особливо коли їхня частота збігається з резонансною частотою провідників на платі [4, 10].

Для боротьби з цими проблемами використовуються різні апаратні методи виявлення помилок. Найпростіший спосіб - це біт парності, коли при передачі кожного байту додається один додатковий біт, який вказує на парність або непарність кількості одиниць у даних. Приймач перевіряє цю парність і може виявити одиночну помилку. Але тут є суттєві обмеження: якщо спотворюються два біти одночасно, парність залишиться правильною і помилка не буде виявлена. До того ж біт парності тільки вказує на наявність помилки, але не дозволяє її виправити [5, 6].

Набагато надійнішим методом є додавання циклічного надлишкового коду, або CRC. Цей алгоритм використовує поліноміальне ділення для створення контрольної суми, яка додається до блоку даних. Дослідження підтверджують, що CRC набагато краще справляється з виявленням множинних помилок і пакетних спотворень порівняно з простою парністю. Саме тому для критичних застосувань рекомендується використовувати CRC замість простого біта парності. Сучасні розробки в галузі завадостійких систем UART пропонують цікаві рішення на рівні

обробки сигналів. Замість того, щоб зчитати стан лінії один раз у середині біта, приймач робить декілька зчитувань і приймає рішення на основі більшості результатів. Такий підхід багатократного зчитування з подальшим аналізом дозволяє системі краще відрізнити корисний сигнал від шуму і зберегти працездатність навіть при значних перешкодах. [2, 3, 4, 6].

Диференціальна передача та кабельна інфраструктура

Якщо говорити про фізичний рівень передачі, то найбільш ефективний спосіб боротьби з електромагнітними перешкодами - це перехід від звичайного однополярного UART (TTL або RS-232) до диференціального інтерфейсу RS-485. Суть диференціальної передачі в тому, що сигнал передається одночасно двома проводами з протилежною полярністю. Коли на лінію наводиться електромагнітна перешкода, вона впливає на обидва проводи приблизно однаково. Приймач же вимірює різницю між сигналами на двох проводах, тому перешкода компенсується і не впливає на результат. Це дає RS-485 чудову стійкість до перешкод і дозволяє передавати дані на відстань до 1200 метрів. Ще одна перевага - можливість працювати навіть при наявності різниці потенціалів землі на кілька вольтів [1, 7, 8].

Для кількісної оцінки, варто порівняти запас завадостійкості. У стандартного 5-вольтового TTL UART він часто складає менше 1 В, що робить його вразливим до будь-яких імпульсних наводок. Натомість RS-485 розроблений для придушення синфазних перешкод - шуму, що наводиться одночасно на обидва сигнальні дроти. Стандартні приймачі RS-485 здатні коректно розпізнавати сигнал при синфазній напрузі в діапазоні від -7В до +12В. Таким чином, стійкість до найпоширенішого типу промислових перешкод зростає не просто в рази, а щонайменше на порядок (в 10-20 разів), порівняно з імпульсом в 1-2В, який може бути фатальним для простого UART.

Драйвери RS-485 створюють диференціальну напругу мінімум 1,5 вольт, а приймачі здатні надійно розпізнавати сигнали від 200 мілівольт. Такий запас забезпечує стабільну роботу навіть при значному ослабленні сигналу через довгий кабель або перешкоди. Не менш важливий аспект - це вибір правильного кабелю та його монтаж. Використання екранованої витой пари суттєво знижує вплив зовнішніх електромагнітних полів. Сам факт скручування проводів вже дає певний захист: в різних частинах кабелю наведені струми мають протилежний напрямок і взаємно компенсуються [1, 8].

Екран додає ще один рівень захисту, але важливо правильно його заземлити. Найкраща практика - заземлювати екран тільки в одній точці, щоб уникнути заземлювальних петель. Якщо заземлити екран з обох кінців кабелю, через нього може потекти струм від різниці потенціалів землі, що тільки погіршить ситуацію. Для особливо критичних застосувань варто додати ще один рівень захисту на програмному рівні. Мається на увазі протокол з підтвердженням отримання даних і повторною передачею при виявленні помилок. Дані передаються пакетами, кожен пакет має контрольну суму або CRC. Якщо приймач виявляє помилку, він запитує повторну передачу конкретного пакета. Така схема значно підвищує надійність, хоча і ускладнює реалізацію та дещо знижує швидкість обміну даними. [3, 9].

Висновки

Досвід показує, що для надійної роботи UART в умовах електромагнітних перешкод потрібен комплексний підхід. Найкращі результати дає поєднання кількох методів: використання CRC замість простої парності для виявлення помилок, застосування алгоритмів багатократного зчитування біта, перехід на диференціальний інтерфейс RS-485 для фізичного рівня, правильний вибір кабелів з екрануванням і скручуванням, а також додавання протоколів підтвердження на рівні програми. Результати досліджень 2024 року підтверджують ефективність такого комплексного підходу. Правильно спроектовані системи UART з багаторівневим захистом демонструють високу надійність і можуть стабільно працювати навіть у складних промислових умовах з високим рівнем електромагнітного забруднення.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Contributors to Wikimedia projects. Rs-485. *Wikipedia*. URL: <https://en.wikipedia.org/wiki/RS-485> (дата звернення: 26.10.2025).
2. Error correction and detection codes. *ElectronicsHub*. URL: <https://www.electronicshub.org/error-correction-and-detection-codes/> (дата звернення: 26.10.2025).
3. For UART, should I use parity on a board level?. *Electrical Engineering Stack Exchange*. URL: <https://electronics.stackexchange.com/questions/9108/for-uart-should-i-use-parity-on-a-board-level> (дата звернення: 26.10.2025).
4. Li R. Development and evaluation of a robust UART communication system with enhanced interference resistance. 29 жовт. 2024 р. URL: <https://doi.org/10.61173/h86z4q46> (дата звернення: 26.10.2025).

5. Parity bit. *Wikipedia*. URL: https://en.wikipedia.org/wiki/Parity_bit (дата звернення: 26.10.2025).
6. Peña E., Legaspi M. G. UART: a hardware communication protocol understanding universal asynchronous receiver/transmitter. *Analog Dialogue*. URL: <https://www.analog.com/en/resources/analog-dialogue/articles/uart-a-hardware-communication-protocol.html> (дата звернення: 26.10.2025).
7. Pini A. UARTs ensure reliable long-haul industrial communications over RS-232, RS-422, and RS-485 interfaces. *DigiKey*. URL: <https://www.digikey.com/en/articles/uarts-ensure-reliable-long-haul-industrial-communications> (дата звернення: 26.10.2025).
8. RS485, specifications and in depth tutorial - Lammert Bies. *Lammert Bies*. URL: <https://www.lammertbies.nl/comm/info/rs-485> (дата звернення: 26.10.2025).
9. Serial communications protocols - part four: RS-485 and baud rates. *Altium*. URL: <https://resources.altium.com/p/serial-communications-protocols-rs-485> (дата звернення: 26.10.2025).
10. What causes UART errors?. *Electrical Engineering Stack Exchange*. URL: <https://electronics.stackexchange.com/questions/83379/what-causes-uart-errors> (дата звернення: 26.10.2025).
11. Yan C. BitDance: Manipulating UART Serial Communication with IEMI. URL: <https://cyansec.com/files/articles/23RAID-BitDance.pdf> (дата звернення: 26.10.2025).

Ішук Владислав Павлович - студент групи РТ-23б, факультет інформаційних електронних систем, Вінницький національний технічний університет, м. Вінниця, e-mail: vlad.ischuck2006@gmail.com

Стальченко Олександр Володимирович - кандидат технічних наук, Вінницький національний технічний університет, м. Вінниця, e-mail: stalchenko.o.v@vntu.edu.ua.

Ishchuk Vladyslav Pavlovych – student of group RT-23b, Faculty of Information and Electronic Systems, Vinnytsia National Technical University, Vinnytsia, e-mail: vlad.ischuck2006@gmail.com

Stalchenko Oleksandr Volodymyrovych - Candidate of Technical Sciences, Vinnytsia National Technical University, Vinnytsia, e-mail: stalchenko.o.v@vntu.edu.ua.