МІНІСТЕРСТВО ОСВІТИ І НАУКИ КРАЇНИ
СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
КОНОТОПСЬКИЙ ІНСТИТУТ

Кафедра електронних
приладів і автоматики

Кваліфікаційна робота бакалавра

СПОСІБ ОТРИМАННЯ ЗАВАДОСТІЙКИХ СИГНАЛІВ ДЛЯ УПРАВЛІННЯ АВТОМАТИЗОВАНОЮ СИСТЕМОЮ

Студент гр. $ЕП_з$-$61_к$ О.С. Голуб

Науковий керівник, В.В. Бібик
доцент,к.ф.-м.н.,

Конотоп 2020 рік

РЕФЕРАТ

Об’єктом дослідження кваліфікаційної роботи є способи отримання завадостійких сигналів для управління автоматизованими системами.

Мета роботи полягає в аналізі видів і джерел завад в автоматизованих системах, а також пошуків шляхів їх усунення.

При виконанні роботи проведено аналіз джерел і видів завад, визначено основні методи підвищення завадостійкості автоматизованих систем.

У результаті проведеного аналізу, встановлено, що існує декілька методів екранування і заземлення елементів та ліній зв’язку в системах автоматики, але найчастіше для зменшення впливу завад на роботу автоматичної системи використовують гальванічну розв’язку

Робота викладена на 32 сторінках, у тому числі включає 17 рисунків, список цитованої літератури із 30 джерел.

КЛЮЧОВІ СЛОВА: ДОСТОВІРНІСТЬ, ЗАЗЕМЛЕННЯ, ШУМИ, ЗАВАДОСТІЙКІСТЬ, ГАЛЬВАНІЧНА РОЗВ’ЯЗКА , GSM/GPRS ТЕХНОЛОГІЇ, ЦИКЛІЧНІ КОДИ, ЕКРАНУВАННЯ.

ЗМІСТ

ВСТУП

Дорогі і надійні контролери, модулі введення-виведення, датчики можуть виявитися непрацездатними, якщо монтаж системи виконаний без урахування вимог електромагнітної сумісності і правил заземлення, а також при невірному методі захисту від впливу перешкод. Наслідком неправильного заземлення можуть бути збої в роботі систем автоматики, підвищена похибка вимірювань, вихід з ладу чутливих елементів, уповільнення роботи системи внаслідок появи потоку завад в каналах обміну, нестабільність регульованих параметрів, помилки в даних, що надходять. [1-11].

Електромагнітні перешкоди - це електромагнітне явище, процес, які знижують або можуть знизити якість функціонування технічного засобу. Для нормального функціонування електронних пристроїв необхідно забезпечувати їх електромагнітну сумісність (ЕМС) з електромагнітної обстановкою (ЕМО) на об'єкті. [1-4] Під електромагнітною обстановкою розуміється сукупність електромагнітних процесів в заданій автоматизованій системі,відповідно, в частотному і часовому діапазоні. [5].

Тема заземлення в промислової автоматизації є недосконало вивчена. Складність проблеми пов'язана з тим, що джерела перешкод, приймачі та шляхи їх проходження розподілені в просторі, момент і факт їх появи часто є випадковою величиною, а місцезнаходження апріорі невідомо. Складно також провести вимірювання перешкод, практично неможливо зробити досить точний теоретичний аналіз, оскільки завдання зазвичай є тривимірним і описується системою диференціальних рівнянь з похідними.

Розуміння причин виникнення перешкод при проектуванні систем автоматизації дозволяє уникнути низки помилок у виборі обладнання, його розміщення, екранування і кабельної розводки, а також прискорити процес впровадження системи. [1]

РОЗДІЛ 1
ЗАВАДИ, ЇХ КЛАСИФІКАЦІЯ І ДЖЕРЕЛА ВИНИКНЕННЯ

1.1 Класифікація завад

Всі перешкоди, що впливають на кабелі, датчики, виконавчі механізми, контролери та металеві шафи автоматики, в більшості випадків протікають у вигляді струму по заземлюючих провідниках, створюючи навколо них паразитне електромагнітне поле і падіння напруги перешкоди на провідниках. Джерелами і причинами перешкод може бути блискавка, статична електрика, електромагнітне випромінювання, "шумляче" обладнання, мережі живлення 220 В 50 Гц, мережеві навантаження, які перемикаються, гальванічні пари, термоелектричний ефект, електролітичні процеси, рух провідника в магнітному полі тощо. [1-6]

Державні центри стандартизації та сертифікації у всіх країнах світу не допускають до виробництва устаткування, що є джерелом перешкод неприпустимо високого рівня. Однак рівень перешкод неможливо зробити рівним нулю. Крім того, на практиці зустрічається досить багато джерел перешкод, пов'язаних з несправностями або використанням не сертифікованого обладнання.

При конструюванні електронної апаратури для зниження рівня перешкод використовують мікропотужну елементну базу з невисокою швидкодією, зменшення довжини провідників і екранування. Особливі заходи вживаються для зниження перешкод від радіопередавальних пристроїв бездротових мереж (докладніше див. Розділ "Промислові мережі та інтерфейси".

Паразитні впливу перешкод на процес передачі сигналу в системах промислової автоматизації можна розділити на наступні групи:

- вплив через кондуктивний зв'язок;
- вплив нееквіпотенціальності "землі";

- наведення через взаємну індуктивність;
- наведення через ємнісні зв'язки;
- високочастотні електромагнітні наводки. [5]

Основною характеристикою перешкоди є залежність спектральної щільності потужності від частоти. Перешкоди, що впливають на системи автоматизації, мають спектр від постійного струму до одиниць гігагерц (рис.1.1).

Рис.1.1. Відносний рівень спектральної щільності потужності і частота основних джерел електромагнітних завад [4]

У сигнальних ланцюгах і ланцюгах заземлення систем автоматизації міститься весь спектр можливих перешкод. Однак вплив надають тільки перешкоди, частоти яких лежать в смузі пропускання систем автоматизації. Середньоквадратичне значення напруги (або струму) перешкоди Епомехі визначається шириною її спектра [5]:

$$E_{\text{помехи}} = \sqrt{\int_{f_н}^{f_в} e^2(f)\, df}, \tag{1.1}$$

де: $e^2(f)$ - спектральна щільність потужності перешкоди, $В^2/Гц$;

$f_н$ і $f_в$ нижня і верхня межі спектра перешкоди. В окремому випадку, коли $e^2(f)$ слабо залежить від частоти, наведене співвідношення спрощується [7]:

$$E_{\text{помехи}} \approx \sqrt{e^2 \cdot (f_в - f_н)}. \tag{1.2}$$

Таким чином, для зменшення впливу перешкод на системи автоматизації потрібно звужувати ширину смуги пропускання ($f_в$ - $f_н$) аналогових модулів введення і виведення. Наприклад, якщо постійна часу датчика τ становить 0,3с, що приблизно відповідає смузі пропускання сигналу:

$$f_{0,7} = 0{,}5 \text{ Гц } (f_{0,7} = 1/2\ \pi \cdot \tau),$$

то обмеження смуги пропускання модуля введення величиною 0,5 Гц дозволить зменшити рівень перешкоди і тим самим підвищити точність вимірювань, знизити вимоги до заземлення, екранування і монтажу системи. Однак фільтр вносить динамічну похибку в результати вимірювання, що залежить від частоти (спектра) вхідного сигналу. [8]

Перешкоди, що лежать в смузі пропускання аналогових систем автоматики, мають частоти до десятків кілогерц. На цифрові ланцюги впливають перешкоди в смузі до сотень мегагерц. Перешкоди гігагерцевого діапазону безпосереднього впливу на системи автоматизації не впливають, проте після перетворення в нелінійних елементах або внаслідок аліасного

ефекту вони можуть породжувати низькочастотні завади, що лежать в межах сприйманого спектра.

Пристрої, в яких відбувається перемикання рівня струму або напруги за короткий проміжок часу, є джерелами широкосмугових завад (двигуни, вимикачі, реле і контактори, трамвайні струмозйомники тошо). Пристрої, в яких відбувається періодична зміна струму або напруги з обмеженою швидкістю наростання, дають вузькосмугові завади (наприклад, стільникові телефони, радіопередавачі, генератори сигналів, мікрохвильові печі, мікропроцесорні системи). [3

Слід зазначити, що наявність фільтра не завжди рятує від впливу перешкод. Наприклад, якщо високочастотна перешкода, перед тим як потрапити на вхід модуля введення, детектується або випрямляється на нелінійних елементах, то з сигналу перешкоди виділяється постійна або низькочастотна складова, яка вже не може бути ослаблена фільтром модуля введення. Як нелінійних елементів можуть виступати, наприклад, контакти різнорідних металів, захисні діоди, стабілітрони, варистори. [1-12]

1.2 Джерела завад

Мережа живлення 220/380 В з частотою 50 Гц і підключені до неї блоки живлення є джерелами наступних перешкод:

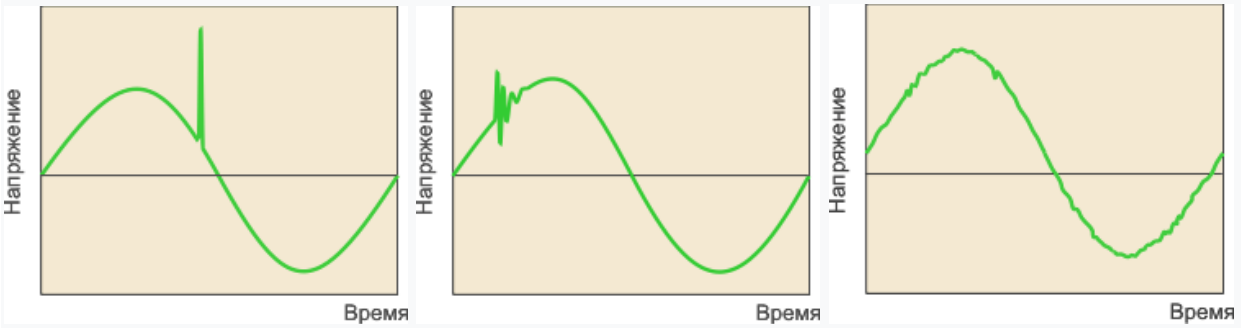
- фон з частотою 50 Гц;

- викиди напруги від розряду блискавки (рис.1.2,а);

- короткочасні затухаючі коливання при перемиканні індуктивного навантаження (рис.1.2, б); [12]

- високочастотний шум (наприклад, перешкода від працюючої радіостанції), накладений на синусоїду 50 Гц (рис.1.2, в);

- інфранизькочастотний шум, що виявляється як нестабільність у часі величини середньоквадратичного значення напруги (рис. 1.3) [11];



а б в

Рис. 1.2. Види перешкод, що проникають з мережі живлення: а - від спалаху блискавки; б - при перемиканні індуктивного навантаження; в - перешкоди від радіостанцій [11]

- довготривалі спотворення форми синусоїди і гармоніки при насиченні сердечника трансформатора і з інших причин.

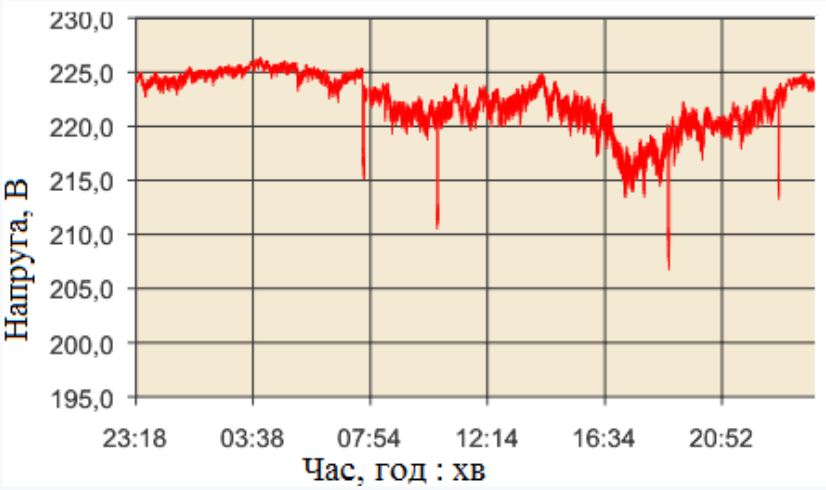


Рис.1.3. Зміни средневипрямленного значення напруги протягом доби [11]

Найбільший вплив на системи промислової автоматики мають перші три види перешкод (рис. 1.3). [13] Для зменшення короткочасних викидів напруги використовують спеціальні захисні діоди і варистори. Інфранізкочастотние шум і спотворення синусоїди фільтруються стабілізатором і згладжує фільтром мережевого джерела живлення і практично не проходять крізь паразитні ємності мережевого трансформатора. Причинами та джерелами мережевих перешкод можуть бути розряди блискавки при попаданні в лінію електропередачі, включення або виключення електроприладів, тиристорні регулятори потужності, реле, електромагнітні клапани, електродвигуни, електрозварювальне обладнання тощо. [3-6]

Шлях струму перешкоди через ємність між первинною обмоткою трансформатора і його заземленим сердечником показаний на рис. 1.4.

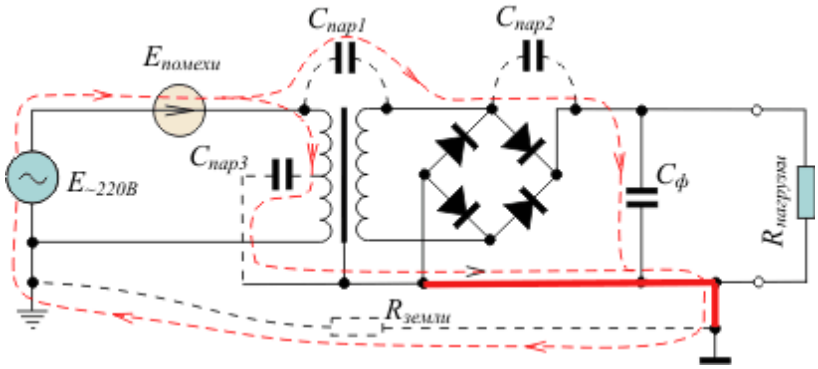


Рис. 1.4. Шляхи проникнення перешкоди із мережі 220 В, 50 Гц в систему заземлення і загальний провід джерела живлення [3]

Цей струм також протікає через загальний провід джерела живлення і заземлювальний провідник. Саме ця ємність є причиною того, що незаземлені електроприлади "б'ють струмом". При відсутності заземлення потенціал металевого корпусу приладів, підключених до мережі 220В, становить від кількох десятків до 220В залежності від опору витоку на землю. Для зменшення цієї напруги корпусу приладів, включених в мережу 220 В, повинні бути заземлені. [7]

РОЗДІЛ 2
МЕТОДИ ЗАХИСТУ ВІД ЗАВАД

2.1 Методи екранування і заземлення елементів автоматизованих систем

До основних методів захисту від завад автоматизованих систем належать [11-19]:

- гальванічно пов'язані ланцюги;
- екранування сигнальних кабелів;
- гальванічно розв'язані ланцюги;
- екрани кабелів на електричних підстанціях;
- екрани кабелів для захисту від блискавки;
- заземлення при диференціальних вимірах;
- інтелектуальні датчики;
- розподілені системи управління;
- чутливі вимірювальні ланцюги тощо.

Недоліком методу поділу провідників заземлення є низька ефективність на високих частотах, коли велику роль грає взаємна індуктивність між рядом йдуть провідниками заземлення, яка тільки замінює гальванічні зв'язку на індуктивні, не вирішуючи проблеми в цілому. [12]

Велика довжина провідників призводить також до збільшення опору заземлення, що важливо на високих частотах. Тому заземлення в одній точці використовується на частотах до 1 МГц, понад 10 МГц заземлювати краще в декількох точках, в проміжному діапазоні від 1 до 10 МГц слід використовувати одноточечну схему, якщо найбільш довгий провідник в ланцюзі заземлення менше 1/20 від довжини хвилі перешкоди.

Для усунення паразитного ємнісного зв'язку і електростатичних зарядів використовують електростатичний екран у вигляді провідної трубки, що

охоплює дроти, екрануються, а для захисту від магнітного поля використовують екран з матеріалу з високою магнітною проникністю. [16]

Оболонку кабелю треба заземлювати з боку джерела сигналу. Якщо заземлення зробити з боку приймача, то струм перешкоди буде протікати через ємність між жилами кабелю, створюючи на ній і, отже, між диференціальними входами, напругу перешкоди. Тому заземлювати оболонку треба з боку джерела сигналу (рис. 2.1). В цьому випадку шлях для проходження струму перешкоди відсутній. Якщо джерело сигналу не заземлене (термопара), то заземлювати екран можна з будь-якого боку, тому що в цьому випадку замкнутий контур для струму перешкоди не утворюється. [19]

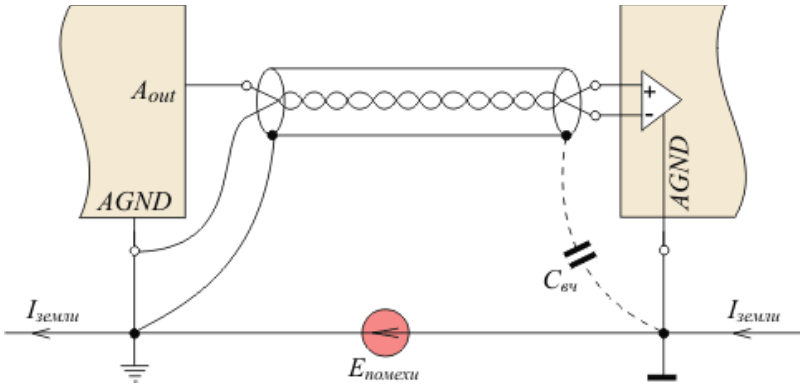


Рис.2.1. Заземлення екрана. Конденсатор використовується для ослаблення високочастотних перешкод [19]

На частотах понад 1 МГц збільшується індуктивний опір екрану і струми ємнісний наведення створюють на ньому велике падіння напруги, яке може передаватися на внутрішні жили через ємність між опліткою і жилами. Крім того, при довжині кабелю, порівнянному з довжиною хвилі перешкоди (довжина хвилі перешкоди при частоті 1 МГц дорівнює 300 м, на частоті 10 МГц - 30 м) зростає опір обплетення, що різко підвищує напругу перешкоди на оболонці. Тому на високих частотах оболонку кабелю треба заземлювати не тільки з обох сторін, але і в декількох точках між ними (рис. 2.2).

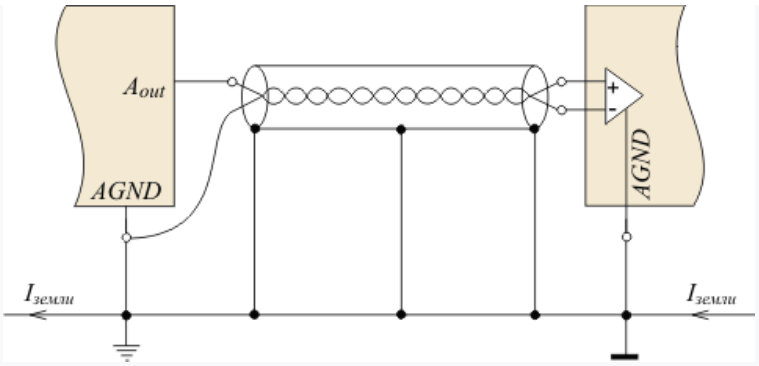


Рис.2.2. Заземлення екрана довгого кабелю на високих частотах [19]

Ці точки вибирають на відстані 1/10 довжини хвилі перешкоди одна від одної. При цьому по оболонці кабелю буде протікати частина струму, що передає перешкоду в центральну жилу через взаємну індуктивність. [12,17]

Оскільки навіть при правильному заземленні, але довгому кабелі перешкода все одно проходить через екран, то для передачі сигналу на велику відстань або при підвищених вимогах до точності вимірювань сигнал краще передавати в цифровій формі або через оптичний кабель.

Екран, що захищає від паразитних індуктивних зв'язків, зробити набагато складніше, ніж електростатичний екран. Для цього потрібно використовувати матеріал з високою магнітною проникністю і, як правило, набагато більшої товщини, ніж товщина електростатичних екранів. Для частот нижче 100 КГц можна використовувати екран зі сталі або пермаллоя. На більш високих частотах можна також використовувати алюміній і мідь.

Радикальним рішенням описаних вище проблем є застосування гальванічного ізоляції з роздільним заземленням цифрової, аналогової і силової частини системи (рис. 2.3). [18]

Застосування гальванічної ізоляції дозволяє розділити аналогову і цифрову землю, а це, в свою чергу, виключає протікання по аналоговій землі струмів перешкоди від силової і цифрової землі (рис. 2.3). Аналогова земля може бути з'єднана з захисним заземленням через опір.

На електричних підстанціях на екрані сигнального кабелю автоматики, прокладеного під високовольтними дротами на рівні землі і заземленого з

одного боку, може наводитися напруга величиною в сотні вольт під час комутації струму вимикачем. Тому з метою електробезпеки екран кабелю заземлюють з двох сторін. [5-12]

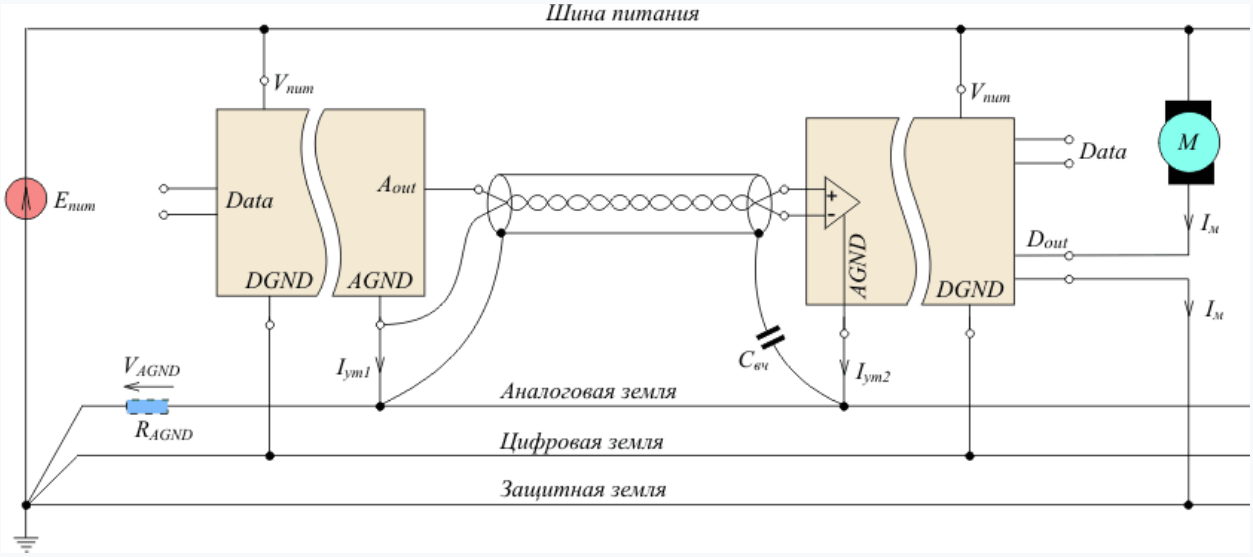


Рис. 2.3. Приклад гальванічно розв'язаного ланцюга [18]

Для захисту від електромагнітних полів з частотою 50 Гц екран кабелю також заземлюють по обидва боки. Це виправдано у випадках, коли відомо, що електромагнітна наводка з частотою 50 Гц більше, ніж наводка, викликана протіканням вирівнюючого струму через екран.

Для захисту від магнітного поля блискавки сигнальні кабелі систем автоматизації, що проходять по відкритій місцевості, повинні бути прокладені в металевих трубах з феромагнітного матеріалу, наприклад, сталі. Труби грають роль магнітного екрана [Vijayaraghavan]. Нержавіючу сталь використовувати не можна, оскільки цей матеріал не є феромагнітним. Труби прокладають під землею, а при наземному розташуванні вони повинні бути заземлені приблизно через кожні 3 метри. [10, 12]

Якщо джерело сигналу не має опору на землю, то при диференціальному вимірі утворюється "плаваючий вхід" (рис. 2.4). На плаваючому вході може наводитися статичний заряд від атмосферної електрики або вхідного струму витоку операційного підсилювача. Для відведення заряду і струму на землю

потенційні входи модулів аналогового введення зазвичай містять в собі резистори опором від 1 МОм до 20 МОм, що з'єднують аналогові входи з землею.

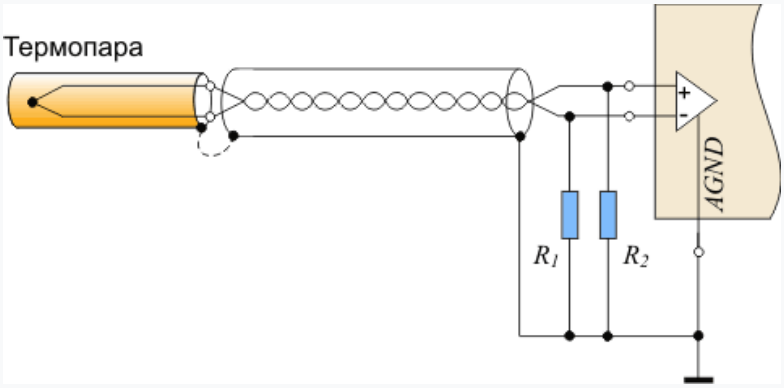


Рис.2.4.Заземлення аналогових входів через опору для зменшення синфазної перешкоди [18]

Однак при великому рівні перешкод або великому опорі джерела сигналу опір 20 МОм може виявитися недостатнім і тоді необхідно додатково використовувати зовнішні резистори опором від десятків кОм до 1 МОм або конденсатори з таким же опором на частоті перешкоди. [4,16]

Останнім часом набули швидке поширення і розвиток так звані інтелектуальні датчики, що містять мікроконтролер для лінеаризації характеристики перетворення датчика Інтелектуальні датчики видають сигнал в цифровий або аналогової формі. Внаслідок того, що цифрова частина датчика поєднана з аналогової, при неправильному заземлення вихідний сигнал має підвищений рівень шуму. На рис.2.5 струм цифровий землі не протікає через опір і тому не вносить шум в напругу сигналу на опорі навантаження.

Деякі датчики мають ЦАП з струмовим виходом і тому вимагають підключення зовнішнього опору навантаження (близько 20 кОм), тому корисний сигнал в них виходить в формі напруги, що падає на навантажувальними резисторами при протіканні вихідного струму датчика.

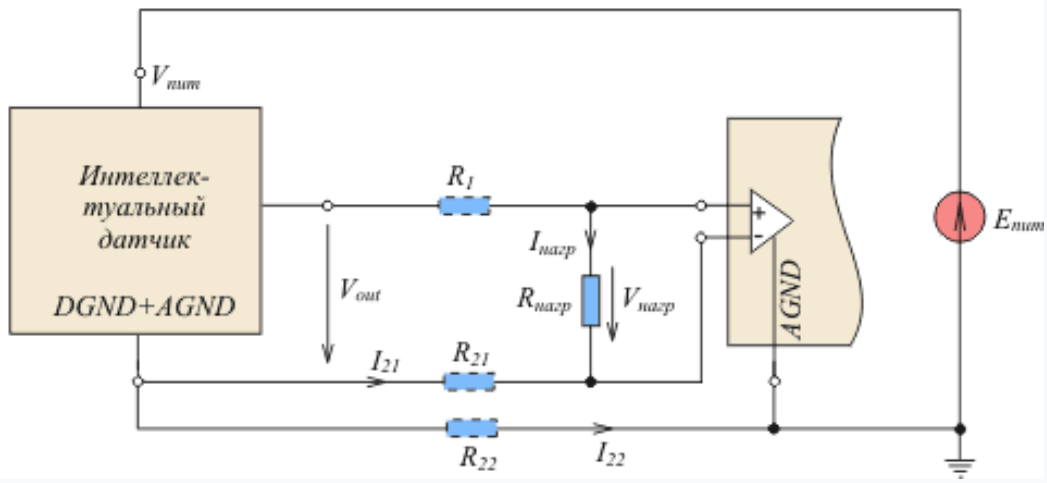


Рис.2.5. Заземлення інтелектуального датчика [16]

Ланцюги живлення двигунів з імпульсним керуванням, двигунів сервоприводів, виконавчих пристроїв з ШІМ-керуванням повинні бути виконані витою парою для зменшення магнітного поля, а також екрановані для зниження електричної компоненти випромінюваної перешкоди. Екран кабелю повинен бути заземлений з одного боку. Ланцюги підключення датчиків таких систем повинні бути поміщені в окремий екран і по можливості просторово віддалені від виконавчих пристроїв. [17]

2.2 Гальванічна розв'язка

Гальванічна розв'язка (ізоляція) ланцюгів є радикальним рішенням більшості проблем, пов'язаних із заземленням, і її застосування фактично стало стандартом в системах промислової автоматизації. Для здійснення гальванічної розв'язки необхідно виконати подачу енергії в ізольовану частину ланцюга і обмін з нею сигналами. Подача енергії виконується за допомогою розв'язує трансформатора (в DC-DC або AC-DC перетворювачів) або за допомогою автономних джерелом живлення: гальванічних батарей і акумуляторів. Передача сигналу здійснюється через оптрони і трансформатори, елементи з магнітним зв'язком, конденсатори або оптоволокно. [20]

Основна ідея гальванічної розв'язки полягає в тому, що в електричному ланцюзі повністю усувається шлях, по якому можлива передача кондуктивної завади. Гальванічна ізоляція дозволяє вирішити наступні проблеми [1,4-22]:

- виключає появи надлишкового електричного струму по шині землі, викликаних різницею потенціалів віддаленох одна від одної земелі, і тим самим знижує індуктивні наведення, викликані цими струмами;

- зменшує практично до нуля напругу синфазної перешкоди на вході диференціального приймача аналогового сигналу (рис. 2.6);

- захищає вхідні і вихідні ланцюги модулів введення і виведення від пробою великою синфазною напругою.

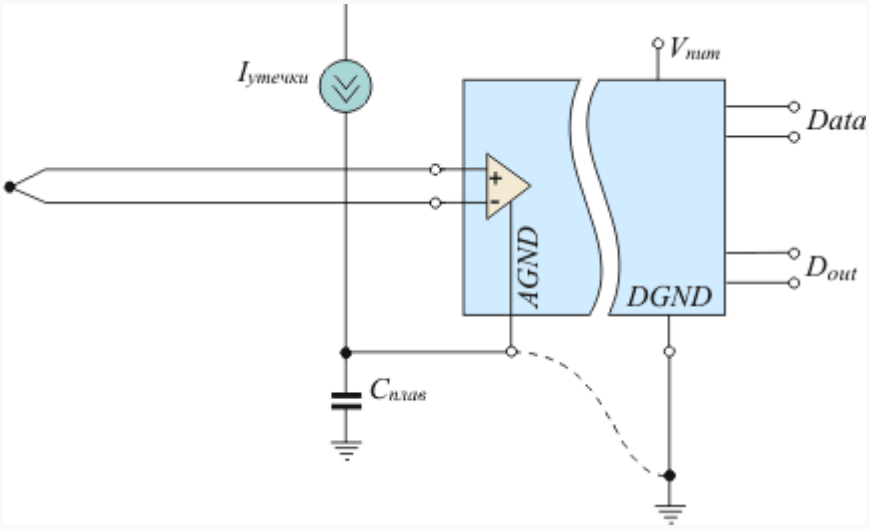


Рис.2.6. Гальванічна розв’язка [20]

Для застосування гальванічної розв'язки система автоматизації ділиться на автономні ізольовані підсистеми, обмін інформацією між якими виконується за допомогою елементів гальванічної розв'язки. Кожна підсистема має свою локальну землю і локальний джерело живлення. Підсистеми заземляють тільки для забезпечення електробезпеки і локального захисту від перешкод. [5,21]

Основним недоліком ланцюгів з гальванічною розв'язкою є підвищений рівень перешкод від DC-DC перетворювача, який, однак, для низькочастотних схем можна зробити досить малим за допомогою цифрової та аналогової фільтрації. На високих частотах ємність підсистеми на землю, а також прохідна ємність елементів гальванічної ізоляції є чинником, що обмежує якість гальвнічно ізольованих систем. Ємність на землю можна зменшити, застосовуючи оптичний кабель і зменшуючи геометричні розміри ізольованої системи. [13-22]

2.3 Захист промислових систем від блискавки

Під час розрядів блискавки з'являється сильне магнітне і електростатичне поле, а також різко підвищується потенціал землі в області заземлення блискавковідводу при ударі блискавки. Всі ці явища призводять до виникнення небезпечних для апаратури напружень на кабелях промислових систем і ланцюгів живлення. [2, 5-8]

Найбільша величина наведення виходить при ударі блискавки в близько розташований блискавковідвід. Оскільки напруженість магнітного поля спадає обернено пропорційно відстані від джерела поля, одним із способів вирішення проблеми може бути віддалення кабелів від громовідводу. Використовуються також електромагнітне екранування, напівпровідникові і газорозрядні захисні елементи.

На рис. 2.7 наведено один з найгірших випадків виникнення великої е.р.с. в кабелі промислової мережі. Неекранована вита пара промислової мережі проходить паралельно блискавковідводу і паралельно шини заземлення, утворюючи контур площу на відстані від громовідводу. Кабель має гальанічну розв'язку із двох сторін. Блискавка наводить в контурі е.р.с., що дорівнює сумі напруг на ємностях пристроїв гальванічної розв'язки і становить величину до декількох кВ. [21]

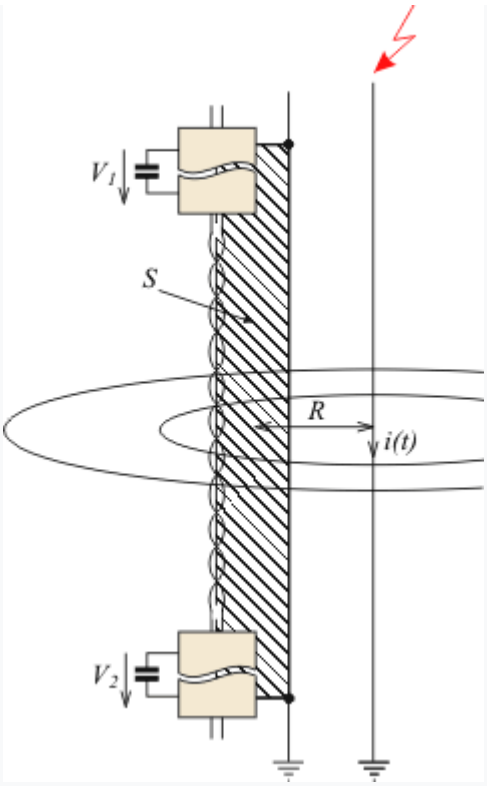


Рис.2.7. Заземлення в промисловій мережі на основі інтерфейсу RS-485 [21]

Оцінимо величину струму, який буде протікати в контурі після пробою ізоляції. Блискавковідвід і заштрихований на рис. 2.7 контур є пов'язаними індуктивностями. При максимальному струмі блискавки 200 кА максимальний струм в контурі буде дорівнює 380 А. Відзначимо, що при діаметрі дроту 1 мм^2 омічний опір контуру складе 0,22 Ом і при е.р.с. в контурі 11 кВ струм короткого замикання був би рівний 50 кА, тобто активним опором контуру можна знехтувати. [2, 4]

Якщо кабель екранований і заземлений з двох сторін, то наведений струм може розплавити дріт заземлення екрана. Якщо екран заземлений з одного боку, то на другому його кінці наводиться напруга в даному прикладі від 800 В до 11 кВ. Такі напруги і струми дійсно виникають в будинках, що не мають в стінах металевої арматури або інших екрануючих поверхонь для захисту від магнітного поля блискавки. [22]

Одним із способів зменшення впливу розрядів блискавки на кабелі є

віддалення громовідводу від будівлі або кабелів від громовідводу. Зокрема, якщо блискавка виникає на великій відстані від кабелів (наприклад, між двома хмарами на висоті 300 м), то в наведеній оцінці струм і напруга наводки будуть приблизно в 100 разів меншими. [23]

Незважаючи на те, що громовідводи розташовані вертикально, в металевих конструкціях будівель, в тому числі в прутах арматури, наведений струм проходить не тільки паралельно блискавковідводу, а й перпендикулярно йому, створюючи магнітне поле в контурах, розташованих не тільки вертикально, але й горизонтально.

Другим наслідком удару блискавки в блискавковідвід є підвищення потенціалу заземлення блискавковідводу і сполученого з ним заземлення будівлі на кілька кВ (рис. 2.8). [24]

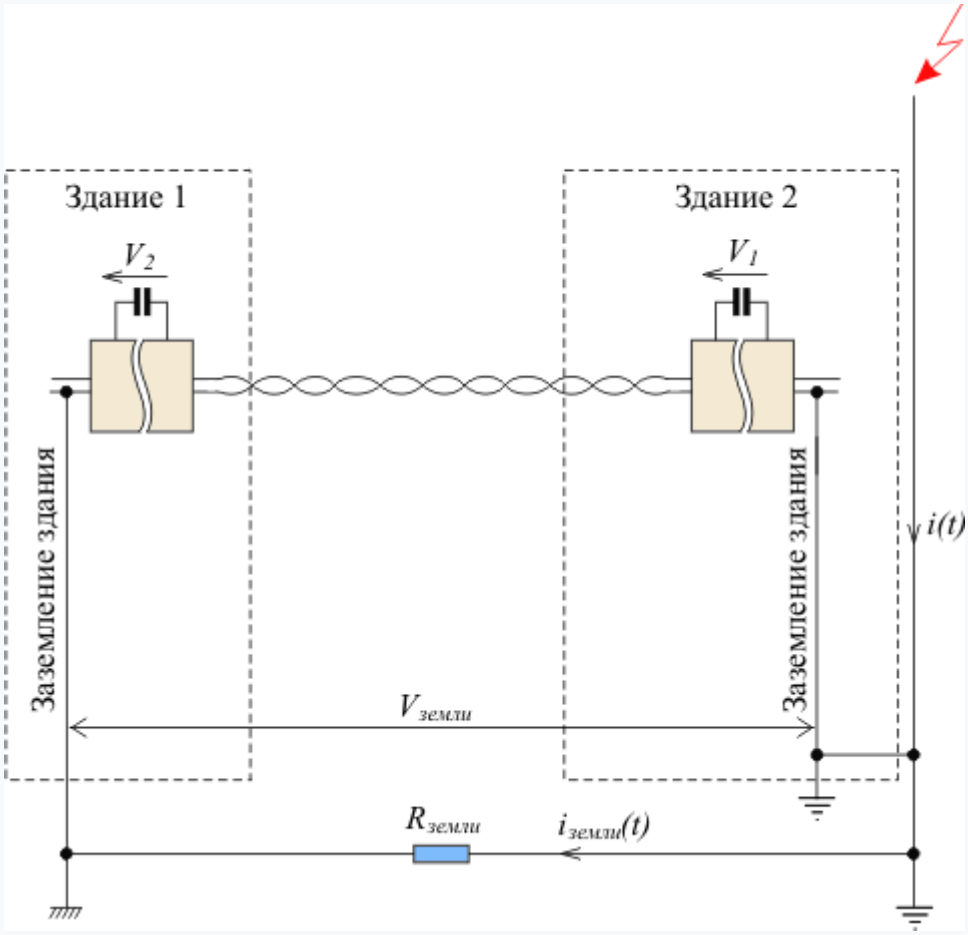
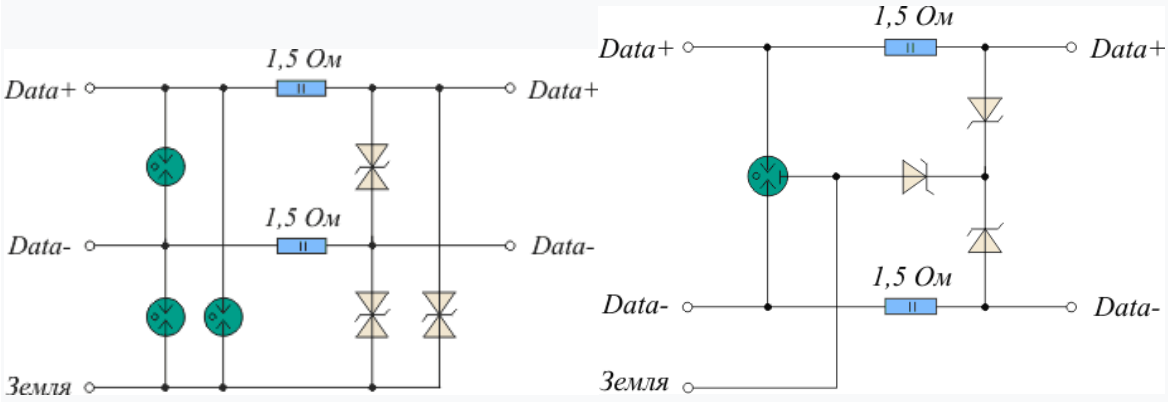


Рис. 2.8. Поява високих напруг на елементах гальванічної розв'язки при ударі блискавки [24]

Якщо при цьому кабель з'єднує інтерфейси систем передачі даних, розташовані в різних будівлях (рис. 2.8), то напруга між заземленими частинами апаратури в різних будівлях може перевищити напруга пробою ізоляції елементів гальванічної розв'язки інтерфейсів. [25]

На рис. 2.9 показані дві схеми побудови ланцюгів захисту для промислової мережі на основі інтерфейсу RS-485. На рис. 2.9, а показана схема на симетричних TVS діодах і двоелектродному газонаповненому розряднику. В якості баластного резистора можуть бути використані позистори, які збільшують свій опір при нагріванні струмом, що протікає.



а б

Рис.2.9. Захист ліній інтерфейсу RS-485 від перенапруг [25]

На рис. 2.9, б показана аналогічна схема, але із застосуванням несиметричних TVS-діодів і трьохелектродного газонаповненого розрядника. Оскільки баластовий резистор включений послідовно з лінією передачі, його опір намагаються зробити по можливості меншим. Частково імпульси перенапруги можна зменшити за допомогою фільтрів на конденсаторах, однак конденсатори часто являють собою неприпустимо великуе ємнісне навантаження для захищається ланцюга. Пристрої захисту різних інтерфейсів і ланцюгів розрізняються напругою спрацьовування (обмеження). Для телефонних ліній це напруга становить 65 В, для Ethernet - 5В, для мереж на основі інтерфейсу RS-485 - 7,5 В. [19-25]

РОЗДІЛ 3
ЗАСТОСУВАННЯ GSM СИГНАЛІЗАТОРІВ ДЛЯ КОНТРОЛЮ МЕРЕЖ ЖИВЛЕННЯ

3.1 GSM / GPRS технології в системах промислової автоматики

Ефект від використання технологій бездротової передачі даних в системах промислової автоматики, на перший погляд, очевидний - економія матеріальних і людських ресурсів, зниження збитків від простою устаткування, збільшення точності вимірювань. Однак цей стандарт передачі даних, крім явних переваг, має також цілий ряд обмежень. Наприклад, використання GSM/GPRS технологій не підходить для потоків даних, критичних по часу доставки. [1, 27]

У той же час, в промислової автоматизації є цілий ряд завдань, які не мають на увазі передачі великих обсягів даних з високою швидкістю. Це завдання диспетчеризації і віддаленого контролю технологічних процесів. На практиці такі системи бездротового моніторингу найчастіше будуються на базі промислових GSM/GPRS модемів. Розглянемо пристрої від провідного виробника індустріального комунікаційного обладнання - компанії MOXA. В [1] для тестування були обрані дві серії модемів промислового застосування: OnCell G2100 і OnCell G3100. [28]

Пристрої OnCell G3100 є «активними» модемами. Їх особливість в тому, що вони можуть самостійно, без подачі зовнішніх команд, встановити GSM / GPRS з'єднаня і виконати передачу даних. Таким чином, до терміналів G3100 можна підключати обладнання, з самого початку не розраховане на передачу даних до модемів. Реалізований в G3100 стек протоколів TCP / IP дозволяє цим модемам передавати дані по технології GPRS через мережі Інтернет або VPN-каналам. [24]

Модеми MOXA підтримують всі основні режими передачі даних, які пропонують вітчизняні оператори настільного зв'язку GSM[25-30]:

- CSD (голосові канали зв'язку);

- GPRS (пакетна передача даних);

- SMS (обмін короткими повідомленнями).

З точки зору користувача, механізм передачі даних по мережах стільникового зв'язку з використанням режиму CSD аналогічний передачі даних по телефонних модемах фіксованого зв'язку. Більш того, допустимим є побудова каналу, на одному кінці якого встановлений GSM-модем, а на іншому - термінал провідного телефонного зв'язку. Технологія CSD забезпечує прозорий канал передачі даних, але вимагає попередньої установки з'єднання (установка проводиться за допомогою АТ-команд).

Функції CSD реалізовані в модеми MOXA серії OnCell G2100. Важливою перевагою застосування CSD є гарантована стандартному GSM пропускна здатність каналу - 9,6 Кбіт/с. Так, результати передачі великих обсягів даних через модеми на швидкостях 9600 біт/с показали можливість стабільно передавати дані з пропускною спроможністю 1021 байт/с, при цьому затримка передачі склала близько 0,6 с. [29]

Технологія обміну короткими повідомленнями SMS і передає пакети даних обсягом до 140 байт. SMS може застосовуватися як в мобільних телефонах, так і в більшості GSM-модемів. Для передачі повідомлення через модем використовується АТ-команда AT + CMGS. "Класична" топологія системи віддаленого управління обладнання по мережах GSM наведена на рис. 3.1. [27]

У модемах MOXA реалізована унікальна функція "SMS Tunnel" забезпечує передачу даних по SMS-каналах без введення спеціальних АТ-команд. Так, будь-яке підключене устаткування може просто передавати дані в звичайному режимі, а модем автоматично буде упаковувати ці дані в SMS-повідомлення і передавати заздалегідь вказаному абоненту.

Рис.3.1. "Класична" топологія системи віддаленого управління обладнання по мережах GSM [27]

Також можливо парне з'єднання модемів, в рамках якого GSM-модеми будуть прозоро передавати дані з одного пристрою на інший за допомогою SMS-повідомлень (рис.3.2).

Рис.3.2. Автоматична установка резервної GSM-зв'язку при використанні "інтелектуального" модему [27]

Функцію SMS Tunnel підтримують обидві серії модемів OnCell. В налаштуваннях функції передбачена можливість вказати один або декілька номерів як для вихідних, так і для вхідних повідомлень, для того, що пристрій брало тільки інформацію тільки від авторизованих абонентів.

Максимальний розмір повідомлення в стандарті GSM - 140 байт. Таким чином, при використанні 7-бітного кодування (латинський алфавіт і цифри) можна відправляти повідомлення довжиною до 160 символів. Тому не рекомендується відправляти пакети даних, довжина яких перевищує обсяг одного SMS-повідомлення: при передачі даних не тільки можуть виникнути паузи, а й може змінитися порядок приходу SMS-повідомлень на приймальній стороні. [6-24]

Серед можливих варіантів застосування режиму SMS Tunnel варто було б виділити системи моніторингу навколишнього середовища, сигналізації та попередження персоналу: при виході контрольованого параметра за межі допустимого значення оператор може отримати відповідне SMS-повідомлення на свій мобільний телефон.

При використанні технології GPRS інформація збирається в пакети і передається через невикористовувані в даний момент голосові канали зв'язку. Як правило, GPRS-пакети мають IP-формат, тому адресація пристроїв GPRS здійснюється не за телефонним номером абонента, а по IP-адресою, а тарифікація даних проводиться не за часом з'єднання, а за обсягом переданих данних. Технологія GPRS дозволяє використовувати кілька голосових каналів одночасно, тобто передавати дані зі швидкістю набагато більшою, ніж в режимі CSD (рис.3.3).

Рис.3.3. Модеми серії MOXA OnCell G2100 [17]

Варто відзначити, що, оскільки пакети GPRS мають формат IP, то дані послідовних інтерфейсів RS-232/422/485 перед передачею повинні бути перетворені в TCP/IP. Підтримка стека TCP/IP може здійснюватися як кінцевим обладнанням, так і модемами. Переваги модемів серії OnCell G3100 в тому, що в них реалізований стек TCP/IP, тому всі завдання по упаковці даних виконує сам модем. Відповідно, до пристроїв G3100 можна підключати будь-яке обладнання з послідовним інтерфейсом, в тому числі з самого початку не призначене для роботи з модемами. [13-16]

Передача даних по GPRS TCP / IP може здійснюватися в двох основних режимах: «парне з'єднання» або «емуляція віртуального COM-порту». При парному поєднанні використовуються два модему G3100: дані, що приходять в один модем, «прозоро» передаються на інший, і навпаки. При емуляції віртуального COM-порту модем може виконувати роль віддаленого послідовного порту комп'ютера. При цьому комп'ютер необхідно підключити до Інтернет (або до VPN-мережі оператора зв'язку), а на комп'ютері встановити драйвер. Після виконання цих нескладних процедур будь-яке програмне забезпечення комп’ютера буде взаємодіяти з віддаленим модемом так само, як і з «рідним» COM-портом. [17-22]

Використання технології GPRS виправдано при необхідності періодичної передачі невеликих обсягів даних. Так, технологія зв'язку GPRS може застосовуватися при віддаленому моніторингу тривало поточних процесів: опитування лічильників, моніторинг температури і вологості навколишнього середовища, контроль рівня рідин, стеження за процесом транспортування нафти і газу і рідини.

Технологія CSD забезпечує прозорий і швидкісний канал передачі даних, але вимагає попередньої установки з'єднання. Це накладає певні обмеження на застосування CSD: обладнання, що використовує цей канал зв'язку, має підтримувати функції роботи з модемами і в потрібний момент видавати команди на установку/призвести до втрати з'єднання. [30]

3.2 Завадостійкість сигналізатора СЗІЦ-Д-Л

Сигналізатори СЗІЦ-Д-Л призначені для контролю опору ізоляції електричної мережі, яка живиться від одного джерела електроживлення. СЗІЦ-Д-Л мають підвищену завадостійкістю і, внаслідок цього, можуть застосовуватися для контролю опору ізоляції лінійних ланцюгів і контролю ланцюгів управління вогнями світлофорів автоблокування при централізованому розміщенні апаратури, найбільш схильних до впливу перешкод. Застосовується в діючих і знову споруджуваних пристроях автоматики і зв'язку (рис.3.4). [23]

Рис.3.4. Сигналізатор заземлення СЗІЦ-Д-Л [23]

Відмітні особливості сигналізатора

- змінено номери контактів для подачі напруги живлення, контрольованої напруги і часом спрацьовування. Дані заходи прийняті для виключення можливості роботи сигналізатора СЗІЦ-Д-Л в посадковому місці сигналізатора СЗІЦ-Д;

- підвищена стійкість до впливу різних видів перешкод, присутніх в лінійних ланцюгах великої довжини;

- наявність додаткового діапазону напруг контрольованого джерела живлення постійного струму (280 +40 В); [22]

- можливість передачі інформації про стан опору ізоляції контрольованої мережі в систему автоматизованого диспетчерського контролю;

- уніфіковане виконання на всі застосовувані види джерел електроживлення;

- цифровий принцип вимірювання опору ізоляції та наявність вбудованого мікропроцесора;

- вбудовані елементи струмового та теплового захисту, що забезпечують пожежну безпеку приладу;

- зменшений вплив нечутливості по полюсах контрольованих джерел живлення постійного струму;

- зменшена нестабільність чутливості при зміні величин контрольованої напруги;

- можливість перевірки працездатності і якісної оцінки величини опору ізоляції без додаткового міліамперметра на місці експлуатації;

- можливість застосування в схемах зміни напряму руху;

- можливість застосування для контролю опору ізоляції кабельних ліній зв'язку та СЦБ. [21-27]

Час спрацювання сигналізатора при підключенні опору витоку із значенням 0,9 від порогового значення:

- не більше 20 с, при контролі ланцюгів постійного струму;

- не більше 4 с, при контролі ланцюгів змінного струму.

Сигналізатор містить цифровий індикатор, що дозволяє оцінювати опір ізоляції цифрами від 0 до 9.

Вихід підключення контрольного реле виконує функції контролю спрацьовування. [28]

ВИСНОВКИ

1. В ході виконання кваліфікаційної роботи було проаналізовано види, джерела походження і характеристики завад в автоматизованих системах. Проблеми перешкод слід починати з пошуку їх джерела. Для цього в першу чергу слід вимірювати рівень перешкод в приймачу сигналу, в джерелі і в сполучному кабелі.

2. Встановлено, що, до основних методів захисту від завад автоматизованих систем належать: гальванічно пов'язані ланцюги; екранування сигнальних кабелів; гальванічно розв'язані ланцюги; екрани кабелів на електричних підстанціях; екрани кабелів для захисту від блискавки; заземлення при диференціальних вимірах; інтелектуальні датчики; розподілені системи управління; чутливі вимірювальні ланцюги гальванічна розв’язка.

3. Використання GSM / GPRS технологій в системах промислової автоматики, а саме CSD (голосових каналів зв'язку); GPRS (пакетної передачі даних); та SMS (обмін короткими повідомленнями) зменшило вплив завад при передаванні і прийманні інформації, збільшило завадостійкість автоматизованих систем контролю.

4. Встановлено, що технології GPRS виправдані при необхідності періодичної передачі невеликих обсягів даних. технологія зв'язку GPRS може застосовуватися при віддаленому моніторингу тривало поточних процесів: опитування лічильників, моніторинг температури і вологості навколишнього середовища, контроль рівня рідин, стеження за процесом транспортування нафти і газу і рідини. Технологія CSD забезпечує прозорий і швидкісний канал передачі даних, але вимагає попередньої установки з'єднання. Це накладає певні обмеження на застосування CSD: обладнання, що використовує цей канал зв'язку, має підтримувати функції роботи з модемами і в потрібний момент видавати команди на установку/призвести до втрати з'єднання.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Paul Horowitz, Winfield Hill. Sztuka elektroniki.– Wydanie siódme: Wydawnictwa Komunikacji i Łączności, Warszawa. – 2003, 509 s.

2. Мичуда З.Р., Мичуда Л.З. Аналоговий багатофункціональний перетворювач. Патент № 89229 Україна, бюл. №1, Оп. 11.01.2010.

3. Мичуда Л.З., Мичуда З.Р. Функціональні перетворювачі рекурентного типу на комутованих конденсаторах для систем енергообліку/ Вісник НУ «Львівська політехніка»: «Теплоенергетика. Інженерія довкілля. Автоматизація.» - Львів. - 2010. - № 677 – с.98-104.

4. Слюсар В.І. Спосіб підвищення швидкості передачі даних сигналами з псевдовипадковою перебудовою частоти.- Заявка на видачу патенту України на корисну модель № u201707800 від 25.07.2017.

5. Зайцев С.В. Інформаційна технологія побудови системи OFDM з внутрібітовою псевдовипадковою перебудовою піднесучих частот в умовах впливу навмисних завад/ С.В. Зайцев, В.В. Приступа, А.В. Яриловець// Вісник Чернігівського державного технологічного університету// № 4 (61), 2012 – С. 131-140

6. Зайцев С.В. Методи та моделі забезпечення сталої достовірності інформації у безпроводових системах передачі даних. Дисертація на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.13.06 – інформаційні технології. - Чернігів – 2016. – 397 с.

7. Золотарев В.В. Помехоустойчивое кодирование. Методы и алгоритмы: справочник/ В.В. Золотарев, Г. В. Овечкин. – М. : Горячая линия – Телеком, 2004. – 126 с.

8. Габидулин Э.М. Кодирование в радиоэлектронике/ Э.М. Габидулин, В.Б. Афанасьев. – М.: Радио и связь, 2016. – 176 с.

9. Morelos-Zaragoza R. The Art of Error Correcting Coding / Morelos-Zaragoza R. – New York: John Wiley & Sons, 2012. – 221 p.

10. Блох Э.Л. Обобщенные каскадные коды/ Э. Л. Блох, В. В. Зяблов. –

М.: Связь, 2016. – 240 с.

11. Скляр Б. Цифровая связь. Теоретические основы и практическое применение/ Скляр. Б. – [2-е изд]. – М.: Вильямс, 2003. – 1104 с. 314

13. Широкополосные беспроводные сети передачи информации/ [В.М. Вишневский, А.И. Ляхов, С.Л. Портной и др.]. – М.: Техносфера, 2015. – 592 с.

14. Hanzo L.L. Adaptive Wireless Transceivers: Turbo-Coded, Turbo Equalized and Space-Time Coded TDMA, CDMA and OFDM Systems/ Hanzo L. L., Wong C.H., Yee M.S. – New York: John Wiley & Sons, 2012. – 738 p.

15. Vishwanath S. Adaptive turbo-coded modulation for flat-fading channels/ S. Vishwanath, A. Goldsmith// IEEE Transactions on Communications. – 2013. – Vol. 51. – P. 964–972.

16. Мальцев А. А. Адаптивное распределение передаваемой мощности в системах радиосвязи с ортогональними поднесущими/ А.А. Мальцев, А.В. Пудеев, А.Е. Рубцов// Вестник ННГУ. – (Серия «Радиофизика»). – 2014. – Вып. 1 (2). – С. 87–96.

17. Letzepis N. Bit error rate estimation for turbo decoding / Nick Letzepis, Alex Grant // IEEE Transactions on Communications. – 2019. – Vol. 57, Issue 3. – P. 585– 590.

19. Квашенников В. В. Методы адаптивной коррекции параметров помехоустойчивого кода и их применение в перспективных системах радиосвязи: дис. доктора техн. наук/ Квашенников Владислав Валентинович. – Владимир, 2010. – 308 с.

20. Peng F. Adaptive Modulation and Coding for IEEE 802.11n / F. Peng, J. Zhang, W. Ryan// Wireless Communications and Networking Conference, (Hong Kong, 11-15 March 2007). – New Jersey, 2007. – P. 656–661.

21. Ergen M. Mobile Broadband. Including WiMax and LTE/ Ergen M. – New York: Springer, 2009. – 513 p.

22. MIMO-OFDM Wireless Communications with Mathlab / [Cho Y., Kim J., Yang W. et al.]. – Singapore : John Wiley & Sons, 2010. – 457 p.

23. Alamouti S. Space-time block coding/ S. Alamouti // IEEE Journal on Selected Areas in Communications. – 2008. – Vol. 16. – P. 1451–1458.

24. Помехозащищенность систем радиосвязи с расширением спектра сигналов методом псевдослучайной перестройки рабочей частоты/ [Борисов В. И., Зинчук В. М., Лимарев А. Е. и др.]. – М. : Радио и связь, 2010. – 384 с.

25. Помехозащищенность систем радиосвязи с расширением спектра сигналов модуляцией несущей псевдослучайной последовательностью/ [Борисов В. И., Зинчук В. М., Лимарев А. Е. и др.]. – М. : Радио и связь, 2013. – 640 с.

26. Помехоустойчивость и эффективность систем передачи информации/ [Зюко А. Г., Фалько А. И., Панфилов И. П. и др.] ; под ред. А. Г. Зюко. – М. : Радио и связь, 2015. – 272 с.

28. Зайцев С. В. Дослідження впливу навмисних завад на пропускну спроможність засобів радіозв'язку з технологією MIMO-OFDM / С. В. Зайцев // Математичні машини і системи. – 2012. – № 1. – С. 139 – 153

29. Zaitsev S. V. Method of estimating reliability of information transmission in wireless networks channels increase in noise and interference / S. V. Zaitsev // International Journal «Information Models and Analyses». – Sofia : ITHEA, 2015. – Vol. 4 (1). – P. 87 – 99.

30. Зайцев С. В. Оцінювання завадозахищеності безпровідних мереж із сигналами OFDM з внутрібітовою псевдовипадковою перебудовою піднесучих частот/ С. В. Зайцев, В.В. Приступа, В.М. Василенко// Вісник Чернігівського державного технологічного університету. – Чернігів : ЧДТУ, 2013. – № 2 (65). – С. 192 – 201.