

## БЕЗПЕКА ПЕРЕДАЧІ ДАНИХ В ПРОМИСЛОВИХ МЕРЕЖАХ СИСТЕМ АВТОМАТИЧНОГО КОНТРОЛЮ ТА УПРАВЛІННЯ

Внаслідок постійної модернізації виробництва, набули широкого застосування системи автоматичного контролю та керування технологічним процесом. Для підтримки та контролю параметрів технологічного процесу застосовуються датчики контролю та виконуючі пристрої, які як правило значно віддалені від керуючого обчислювального засобу. В реальних умовах фабрики віддаленість пунктів контролю та управління досягає 700 - 1 000 м, а лінії зв'язку проходять в безпосередній близькості з високовольтними лініями живлення обладнання фабрики.

Для організації промислових мереж використовують протоколи Modbus, Ethernet, CAN, HART, Profibus та інші. Вони забезпечують зв'язок нижнього та верхнього рівнів автоматизованих систем управління технологічними процесами. Протоколи розробляються з урахуванням особливостей виробництва та технічних систем, забезпечуючи надійне з'єднання та високу точність передачі між віддаленими пристроями. Поряд із надійністю роботи в жорстких умовах все більш важливими вимогами в системах стають функціональні можливості, гнучкість у побудові, простота інтеграції, розширення та обслуговування.

Незважаючи на свій вік, Modbus не тільки втратив актуальність, але навпаки, суттєво зросла кількість нових розробок та обсяг організаційної підтримки цього протоколу.

Перевагами протоколу Modbus є відсутність необхідності у спеціальних інтерфейсних контролерах та простота програмної реалізації. Він дозволяє уніфікувати команди обміну завдяки стандартизації номерів (адрес) реєстрів та стандартизації функцій їх читання та запису.

Головним недоліком даного протоколу є мережевий обмін на кшталт «головний/підлеглий», що дозволяє дозволеним підлеглим пристроям передавати дані головному у міру їх появи.

Протокол Modbus широко використовується для передачі даних послідовною лінією зв'язку, заснованої на інтерфейсах RS-485, RS-422, RS-232. В даний час інтерфейс RS-485 дозволяє об'єднувати кілька пристроїв в єдину мережу і досягти більш високої швидкості передачі на великі відстані.

Протокол Modbus передбачає, що тільки один провідний пристрій і до 247 підлеглих можуть бути об'єднані в промислову мережу. Обмін даними ініціюється головним. Підлегли пристрої не починають передачу даних доти, доки не отримають запит від ведучого. Підлегли пристрої також можуть обмінюватися даними один з одним. Тому будь-якої миті часу в мережі Modbus може відбуватися лише один акт обміну.

Пакет даних у Modbus виглядає наступним чином:

**Адреса (1 байт) | Код функції (1 байт) | Дані (0 ... 252 байта) | Контрольна сума (2 байта).**

Поле «Контрольна сума» є важливим елементом протоколу, яке містить інформацію, необхідну для перевірки цілісності повідомлення та відсутності помилок передачі.

Помилки зв'язку зазвичай полягають у зміні біта або біт повідомлення, які виявляються за допомогою символу кадру, контролю парності та надмірного кодування.

Коли виявляється помилка кадрування, парності і/або контрольної суми, обробка повідомлення пристроєм припиняється. Підлеглий не повинен генерувати повідомлення у відповідь. Алгоритм роботи головного пристрою повинен розроблятися так, щоб у разі не отримання повідомлення у відповідь протягом певного часу (або отримання пакету з помилкою), виконується фіксація помилки зв'язку, ретрансляція повторно повідомлення і коректа її обробка, процесів, а також власних критеріїв агентів даної системи.

### Список літератури

1. **К. Hiroyoshi** FCS Compact Control Station in CENTUM CS R3/ **Hiroyoshi K.**// Yokogawa Technical Report, No. 38,2004, pp. 5-8;
2. **С. Palmer, S. Sheno**i Critical Infrastructure Protection / **Palmer C., Sheno**i S.//III: Third IFIP WG 11. 10 International Conference, Hanover, New Hampshire, USA, March 23-25, 2009, page 87.