**-Modbus RTU**

Modbus RTU (Remote Terminal Unit) là một trong các biến thể của giao thức Modbus, một giao thức truyền thông được sử dụng rộng rãi trong ngành công nghiệp để kết nối và truyền thông giữa các thiết bị điều khiển và cảm biến. Modbus RTU hoạt động dựa trên việc truyền dữ liệu dưới dạng các gói tin nhị phân qua cổng COM (RS-232) hoặc RS-485.

Các đặc điểm quan trọng của Modbus RTU bao gồm:

1. **Phương thức truyền thông dựa trên giao thức master/slave:** Trong một mạng Modbus RTU, có một thiết bị master (hoặc máster) kiểm soát giao tiếp và các thiết bị slave (hoặc slaves) thực hiện theo chỉ thị của master.
2. **Truyền thông serial:** Modbus RTU thường sử dụng cổng COM RS-232 hoặc RS-485 cho việc truyền dữ liệu giữa các thiết bị.
3. **Khung dữ liệu:** Dữ liệu được truyền bằng cách sử dụng các khung dữ liệu định dạng Modbus RTU, bao gồm địa chỉ của thiết bị, mã chức năng (function code) để chỉ định loại hoạt động, dữ liệu và kiểm tra lỗi.
4. **Địa chỉ thiết bị:** Mỗi thiết bị trong mạng Modbus RTU có một địa chỉ duy nhất để được phân biệt.
5. **Chức năng đa dạng:** Modbus RTU hỗ trợ một loạt các chức năng bao gồm đọc và ghi dữ liệu từ và đến các thiết bị slave, điều khiển và kiểm soát các thiết bị.
6. Cấu trúc bảng tin: Một bản tin Modbus RTU bao gồm: 1 byte địa chỉ  –  1 byte mã hàm – n byte dữ liệu – 2 byte CRC

A diagram of a computer program

Description automatically generated

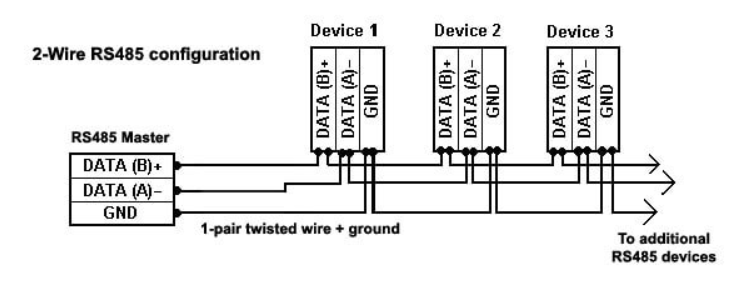
Chức năng và vai trò cụ thể:

* **Byte địa chỉ**: xác định thiết bị mang địa chỉ được nhận dữ liệu (đối với Slave) hoặc dữ liệu nhận được từ địa chỉ nào (đối với Master). Địa chỉ này được quy định từ 0 – 254
* **Byte mã hàm**: được quy định từ Master, xác định yêu cầu dữ liệu từ thiết bị Slave. Ví dụ mã 01: đọc dữ liệu lưu trữ dạng Bit, 03: đọc dữ liệu tức thời dạng Byte, 05: ghi dữ liệu 1 bit vào Slave, 15: ghi dữ liệu nhiều bit vào Slave …
* **Byte dữ liệu**: xác định dữ liệu trao đổi giữa Master và Slave.
  + Đọc dữ liệu:
    - Master:  2 byte địa chỉ dữ liệu – 2 byte độ dài dữ liệu
    - Slave: 2 byte địa chỉ dữ liệu – 2 byte độ dài dữ liệu – n byte dữ liệu đọc được
  + Ghi dữ liệu:
    - Master: 2 byte địa chỉ dữ liệu  – 2 byte độ dài dữ liệu – n byte dữ liệu cần ghi
    - Slave: 2 byte địa chỉ dữ liệu – 2 byte độ dài dữ liệu
* **Byte CRC**: 2 byte kiểm tra lỗi của hàm truyền. cách tính giá trị của Byte CRC 16 Bit

Modbus RTU thường được sử dụng trong các ứng dụng công nghiệp như điều khiển thiết bị tự động, giám sát, thu thập dữ liệu từ cảm biến và thiết bị đo lường. Nó là một giao thức truyền thông đơn giản và hiệu quả cho các ứng dụng như thiết bị điều khiển và tự động hóa công nghiệp.

* **RS485**

RS485 là một chuẩn truyền thông được xây dựng trên nền tảng chuẩn RS422. Điểm khác biệt chính là RS485 cho phép tối đa 32 cặp thu phát có mặt trên đường truyền cùng lúc. Tương tự, RS485 cũng một trở kháng 120 Ohm ở cuối đường truyền để ngăn chặn tín hiệu phản xạ và giao thoa. Nếu có nhiều hơn một thiết bị cần truyền dữ liệu, thì đường RTS được sử dụng như một đường điều khiển, cho phép truyền dữ liệu. RS-485 là một giao thức truyền thông và một giao diện điện trung bình được sử dụng rộng rãi trong ứng dụng công nghiệp để kết nối và truyền dữ liệu giữa các thiết bị điện tử qua một mạng. Dưới đây là một số điểm quan trọng về RS-485:



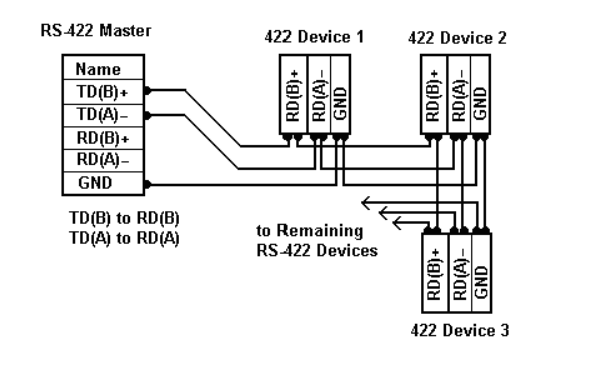
* Up to 32 Driver/Receiver Pairs
* Chiều dài đường truyền và tốc độ tối đa cho phép:
  + 40 Feet = 12m 10 Mbits/sec
  + 400 Feet = 122m 1 Mbits/sec
  + 4000 Feet = 1219m 100 kbits/sec
  + Mức tín hiệu:

Với  hai  dây A, B truyền dẫn cân bằng, tín hiệu mức cao TTL được quy định khi áp của dây A lớn hơn dây B tối thiểu là 200mV, tín hiệu mức thấp TTL được quy định khi áp của dây A nhỏ  hơn dây B tối thiểu cũng là 200mV. Nếu điện áp VAB mà nằm trong khoảng  -200mV < VAB<  200mV thì tín hiệu lúc này được xem như là rơi vào vùng bất định. Điện thế  của mỗi dây tín hiệu so với mass bên phía thu phải nằm trong khoảng –7V đến +12V.

1. **Giao diện điện:** RS-485 là một giao diện điện, cụ thể là một chuẩn kỹ thuật về tín hiệu điện để truyền dữ liệu. Nó sử dụng dây cặp xoắn (twisted pair) để truyền tín hiệu điện qua mạng.
2. **Mạng nhiều điểm:** RS-485 hỗ trợ mạng nhiều điểm, có nghĩa rằng nó cho phép nhiều thiết bị được kết nối vào cùng một mạng và truyền dữ liệu qua cùng một đường truyền. Mạng RS-485 có thể bao gồm một máster và nhiều slaves.
3. **Truyền thông điểm-điểm hoặc nhiều điểm-điểm:** RS-485 có thể được cấu hình để truyền thông điểm-điểm (point-to-point) hoặc nhiều điểm-điểm (multi-point). Trong trường hợp truyền thông nhiều điểm-điểm, các thiết bị slave có thể trả lời truy vấn từ thiết bị master.
4. **Độ xa:** RS-485 cho phép truyền dữ liệu trên một khoảng cách xa, thậm chí lên đến hàng trăm mét, mà không cần đệm lại tín hiệu.
5. **Khả năng chống nhiễu:** RS-485 được thiết kế để chống nhiễu điện từ và nhiễu elektromagnetik, làm cho nó phù hợp cho môi trường công nghiệp nơi nhiễu điện và nhiễu từ là thách thức.
6. **Tốc độ truyền dữ liệu:** RS-485 hỗ trợ các tốc độ truyền dữ liệu khác nhau, từ chậm đến nhanh, tùy thuộc vào thiết bị và ứng dụng cụ thể.
7. **Giao thức truyền thông khác:** RS-485 là giao diện vật lý và không định nghĩa giao thức truyền thông cụ thể. Giao thức như Modbus RTU, Profibus, và BACnet thường được triển khai trên mạng RS-485 để đảm bảo truyền thông giữa các thiết bị.

* **RS422**

RS422 là một chuẩn truyền thông được phát triển bởi “Electronic Industry Association” và “Telecommunications Industry Association” (EIA/TIA); thường được gọi tắt là RS422 hay RS-422 thay vì EIA/TIA-422. Chuẩn này chỉ đề cập đến việc truyền dữ liệu nối tiếp giữa một host (DTE-Data Terminal Equipment) và một ngoại vi (DCE-Data Circuit-Terminating Equipment). RS-422 là một giao diện truyền thông chuẩn được sử dụng rộng rãi trong ứng dụng công nghiệp và truyền dữ liệu điểm-điểm (point-to-point) hoặc điểm-nhiều điểm (multi-point) qua dây cặp xoắn (twisted pair). Dưới đây là một số điểm quan trọng về RS-422:



* Tiêu chuẩn : TIA/DTE-422
* Phương tiện vật lý : Cáp xoắn đôi
* Cấu trúc mạng : liên kết điểm – điểm , liên kết điểm đa – đa điểm
* Khoảng cách truyền tối đa : 1200m (4000 ft)
* Tốc độ truyền tối đa : 100KBS -10MBS
* Mức điện áp : – 6V đến + 6V (điện áp chênh lệch cực)
* Tín hiệu khả dụng : Tx +, Tx-, Rx +, Rx- (Full duplex)
* 1 Driver up to 10 Receivers
* Chiều dài đường truyền và tốc độ tối đa:
  + 40 Feet = 12m 10 Mbits/sec
  + 400 Feet = 122m 1 Mbits/sec
  + 4000 Feet = 1219m 100 kbits/sec

Chuẩn truyền thông RS-422 là một chuẩn truyền thông nối tiếp (serial). RS-422 hỗ trợ truyền thông tốc độ cao và khoảng cách truyền dữ liệu dài. Mỗi tín hiệu được truyền trên một cặp dây ( 2 dây) và đó là sự khác biệt với các chuẩn truyền thông khác RS-422 là một cơ chế vận chuyển phổ biến cho các bộ mở rộng RS-232. Chúng bao gồm các cổng RS-232 ở hai đầu của kết nối RS-422.

Với khoảng cách 40 feet ( tương đương 12m) thì tốc độ truyền dữ liệu tối đa là 100 Kilobytes trên giây. Một điện trở 120 – Ohm được mắc nối tiếp ở cuối đường truyền để ngăn chặn tín hiệu phản xạ và giao thoa. RS422 thường được sử dụng giữa một cặp thu phát này và một cặp thu phát khác.

Tuy nhiên, ở mỗi đầu ra, có thể truyền tới tối đa 10 đầu nhận.

Chuẩn này bao gồm máy thu vi sai, trình điều khiển vi sai và tốc độ dữ liệu cao tới 10 Megabits mỗi giây ở tốc độ 12 mét (40 ft).Vì chất lượng tín hiệu suy giảm theo chiều dài cáp, tốc độ dữ liệu tối đa giảm khi chiều dài cáp tăng.

1. **Cấu trúc dây cặp xoắn:** RS-422 sử dụng hai dây dẫn điện, một dây là "TX+" (truyền dữ liệu từ thiết bị gửi) và một dây là "TX-" (truyền dữ liệu từ thiết bị nhận). Điều này tạo ra một cặp dây xoắn được sử dụng để truyền tín hiệu. Do đó, RS-422 thường được gọi là "cân bằng" (balanced) vì nó sử dụng cặp dây xoắn, trong đó cả hai dây đều truyền tín hiệu, và nó giúp giảm nhiễu và nhiễu crosstalk.
2. **Độ xa và tốc độ truyền dữ liệu:** RS-422 cho phép truyền dữ liệu trên khoảng cách xa hơn so với RS-232, thậm chí có thể đạt đến hàng trăm mét. Nó cũng hỗ trợ các tốc độ truyền dữ liệu nhanh, từ vài kbps đến hàng Mbps, tùy thuộc vào thiết bị và ứng dụng cụ thể.
3. **Giao thức truyền thông:** RS-422 là một giao diện vật lý và không định nghĩa giao thức truyền thông cụ thể. Một giao thức như RS-232 hoặc RS-485 có thể được triển khai trên cơ sở RS-422 để đảm bảo truyền thông giữa các thiết bị.
4. **Ứng dụng:** RS-422 thường được sử dụng trong các ứng dụng yêu cầu truyền dữ liệu trên khoảng cách xa và chất lượng tín hiệu tốt, như trong hệ thống kiểm soát tự động, hệ thống giám sát, và truyền dữ liệu từ cảm biến và thiết bị đo lường.
5. **Cấu hình:** RS-422 có thể được sử dụng trong các cấu hình point-to-point (điểm-điểm) hoặc multi-point (điểm-nhiều điểm). Trong cấu hình multi-point, một thiết bị gửi có thể giao tiếp với nhiều thiết bị nhận, nhưng nó yêu cầu cấu hình đặc biệt để tránh xung đột dữ liệu.
6. **Chống nhiễu:** Tương tự như RS-485, RS-422 cũng có khả năng chống nhiễu tốt hơn so với RS-232, giúp đảm bảo truyền dữ liệu ổn định trong môi trường công nghiệp có nhiễu điện và nhiễu elektromagnetik.
7. **Ưu nhược điểm:**

RS-422 tương tự như giao thức RS-232 và có thể được thiết lập theo cùng một cách, tuy nhiên, nó vẫn có một vài ưu điểm và nhược điểm khác nhau.Tốc độ truyền của RS-422 nhanh hơn và có khả năng đa điểm. Ngoài ra, bạn có thể thấy rằng có ít thiết bị hỗ trợ RS422 hơn. Một số ưu điểm là:

* Chạy đường dài – Thường được hỗ trợ lên đến 500 feet và với các bộ lặp, thậm chí có thể đạt được khoảng cách xa hơn. Multi-Drop – Thông thường, có thể kết nối tối đa 32 thiết bị trên mỗi cổng và thậm chí nhiều hơn bằng cách sử dụng các bộ lặp.
* Chống ồn – Vì nó sử dụng cặp truyền và nhận FLOATING riêng biệt (bốn dây), nó cung cấp khả năng chống ồn tốt hơn so với RS232.
* Multi-Drop – Thông thường, có thể kết nối tối đa 32 thiết bị trên mỗi cổng và thậm chí nhiều hơn bằng cách sử dụng các bộ lặp. Các thiết bị được phân biệt bởi các địa chỉ duy nhất được gán cho từng thiết bị. Ví dụ: nếu bạn có 5 thiết bị được gắn vào một cổng, chúng sẽ được xử lý từ đơn vị 1 đến 5. Nếu bạn muốn liên lạc với đơn vị số 1, bạn gửi lệnh đến đơn vị số 1. Tất cả các đơn vị NGHE lệnh, nhưng chỉ đơn vị địa chỉ sẽ trả lời. Điều này cũng áp dụng cho RS485. Các địa chỉ có thể được đặt qua các công tắc hoặc phần mềm, tùy thuộc vào thiết kế của thiết bị
* **Xây dựng cấu trúc đơn giản**

Cấu trúc bản tin RS-485 với kiểm tra lỗi 16-bit thường sử dụng một phần tiêu chuẩn của giao thức Modbus RTU. Đây là một ví dụ về cấu trúc bản tin Modbus RTU với kiểm tra lỗi 16-bit:

Start bit: @

1byte địa chỉ:

* 0 (master)
* 1 (slave 1)
* 2 (slave 2)
* 3 (PC)

1 byte chức năng:

* 0 đọc theo 1 bit
* 1 ghi theo 1 bit
* 2 đọc theo 1 byte
* 3 ghi theo 1 byte

N byte dữ liệu:

* 1 byte đầu là độ dài n byte dữ liệu
* N byte sau là n byte dữ liệu cần đọc

2 byte check sum:

* Lấy n + địa chỉ + mã hàm

1 byte stop: #

1. Địa chỉ thiết bị (1 byte): Đây là địa chỉ của thiết bị trên mạng RS-485. Mỗi thiết bị có một địa chỉ duy nhất.
2. Mã chức năng (1 byte): Mã chức năng xác định hoạt động mà bản tin yêu cầu thực hiện, ví dụ: đọc đầu vào, ghi đầu ra, v.v.
3. Dữ liệu (n byte): Phần này chứa dữ liệu cụ thể cho yêu cầu hoặc phản hồi. Số lượng byte dữ liệu có thể thay đổi tùy thuộc vào mã chức năng và loại yêu cầu.
4. Kiểm tra lỗi CRC-16 (2 byte): Kiểm tra lỗi CRC-16 được tính từ địa chỉ thiết bị đến phần cuối của dữ liệu. CRC-16 được tính để kiểm tra tính toàn vẹn của bản tin.

* Hàm kiểm tra lỗi

uint16\_t modbus\_crc16 (const uint8\_t\* buf, int len) {

uint16\_t crc = 0xFFFF;

for (int pos = 0; pos < len; pos++) {

crc ^= (uint16\_t)buf[pos]; // XOR byte vào CRC

for (int i = 8; i != 0; i--) { // 8 bits trong 1 byte

if (crc & 0x0001) { // Kiểm tra bit cuối cùng (LSB) của CRC

crc >>= 1; // Dịch phải 1 bit

crc ^= 0xA001; // XOR với 0xA001 (Đa thức CRC-16 Modbus)

} else {

crc >>= 1; // Dịch phải 1 bit

}

}

}

return crc;

}

master

slave

Sensor

PC