

(۱)

پروتکل HART (Highway Addressable Remote Transducer) یک پروتکل ارتباطی صنعتی است که برای ارتباط با ابزار دقیق هوشمند مانند ترانسمیترها، شیرهای کنترلی، فشارسنج‌ها و سایر تجهیزات صنعتی استفاده می‌شود. این پروتکل ترکیبی از سیگنال‌های آنالوگ و دیجیتال را برای ارسال و دریافت داده‌ها به کار می‌برد و امکان نظارت و پیکربندی تجهیزات را از راه دور فراهم می‌کند.

چرایی توسعه پروتکل HART

۱. نیاز به ارتباط دیجیتال در کنار سیگنال‌های آنالوگ در صنایع مختلف، کنترل فرایندها معمولاً با استفاده از سیگنال ۴-۲۰ میلی‌آمپر انجام می‌شد. اما این سیگنال فقط یک مقدار اندازه‌گیری شده را منتقل می‌کرد و امکان ارسال اطلاعات بیشتر (مانند وضعیت دستگاه، تنظیمات کالیبراسیون، تشخیص خرابی و غیره) وجود نداشت. HART برای حل این مشکل، ارتباط دیجیتال روی سیگنال آنالوگ موجود را امکان‌پذیر کرد.

۲. سازگاری با تجهیزات قدیمی از آنجایی که بسیاری از سیستم‌های صنعتی از سیگنال ۴-۲۰ میلی‌آمپر استفاده می‌کنند، تغییر کامل به سیستم‌های دیجیتال هزینه‌بر و دشوار بود. HART به عنوان یک پروتکل هیبریدی توسعه یافت تا با زیرساخت‌های قدیمی سازگار باشد و بدون تغییر اساسی در تجهیزات، قابلیت‌های دیجیتال را اضافه کند.

۳. قابلیت ارتباط دوطرفه و تشخیص خطا برخلاف سیستم‌های آنالوگ که فقط مقدار اندازه‌گیری را ارسال می‌کردند، HART امکان ارتباط دوطرفه را فراهم کرد، به طوری که می‌توان تنظیمات تجهیزات را از راه دور تغییر داد یا داده‌های تشخیصی را از آن‌ها دریافت کرد.

۴. کاهش هزینه‌های تعمیر و نگهداری با استفاده از قابلیت‌های نظارتی HART، می‌توان تجهیزات را از راه دور پایش و عیب‌یابی کرد. این امر باعث کاهش زمان توقف سیستم، افزایش بهره‌وری و کاهش هزینه‌های تعمیر و نگهداری می‌شود.

کاربردهای اصلی پروتکل HART

- ✓ اندازه‌گیری و کنترل فرآیندها – در صنایعی مانند نفت و گاز، پتروشیمی، نیروگاه‌ها، تصفیه آب و فاضلاب برای نظارت بر فشار، دما، سطح و جریان استفاده می‌شود.
- ✓ کالیبراسیون و تنظیم تجهیزات – امکان کالیبراسیون سنسورها و تنظیم پارامترهای عملیاتی از راه دور.
- ✓ تشخیص و عیب‌یابی پیشرفته – ارسال هشدارها و داده‌های تشخیصی برای شناسایی مشکلات تجهیزات پیش از خرابی کامل.
- ✓ یکپارچه‌سازی با سیستم‌های SCADA و DCS - برای انتقال داده‌های دقیق به سیستم‌های نظارتی و کنترلی پیشرفته.
- ✓ افزایش بهره‌وری و کاهش زمان توقف سیستم‌ها – به دلیل امکان انجام تنظیمات بدون نیاز به توقف فرآیند.

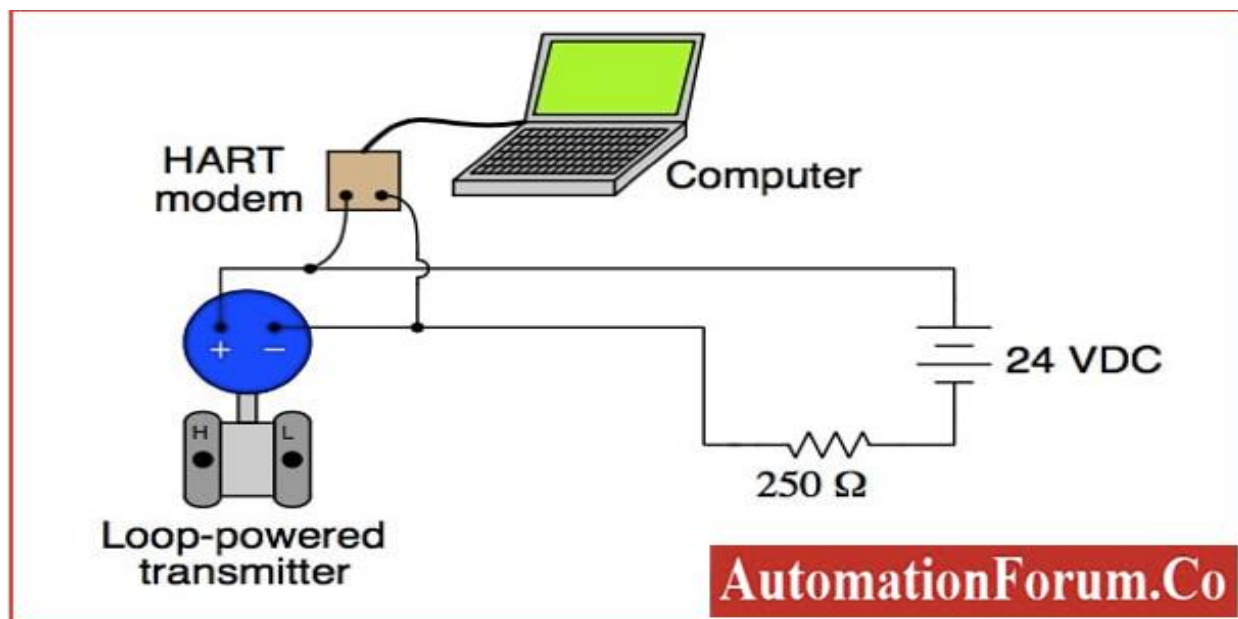
(۲)

لایه فیزیکی پروتکل HART

در لایه فیزیکی، پروتکل HART از سیگنال آنالوگ ۴-۲۰ میلی‌آمپر به عنوان حامل اصلی استفاده می‌کند و داده‌های دیجیتال را با استفاده از مدولاسیون FSK بر روی این سیگنال سوار می‌کند. در این روش، دو فرکانس ۱۲۰۰ هرتز و ۲۲۰۰ هرتز به ترتیب برای نمایش بیت‌های '۱' و '۰' استفاده می‌شوند. این سیگنال‌های فرکانسی با دامنه کم به سیگنال آنالوگ اضافه می‌شوند، بدون اینکه در اندازه‌گیری‌های آنالوگ اختلال ایجاد کنند.

مدار لایه فیزیکی پروتکل HART

مدار لایه فیزیکی پروتکل HART شامل یک منبع جریان ۴-۲۰ میلی‌آمپر است که به صورت سری با یک مقاومت ۲۵۰ اهمی و دستگاه اندازه‌گیری (مانند ترانسمیتر) قرار می‌گیرد. سیگنال دیجیتال با استفاده از مدولاسیون FSK بر روی سیگنال آنالوگ سوار می‌شود و از طریق همین دو سیم منتقل می‌شود.



استفاده از سیگنالینگ تفاضلی

پروتکل HART از سیگنالینگ تفاضلی استفاده نمی‌کند. در عوض، از مدولاسیون FSK برای انتقال داده‌های دیجیتال بر روی سیگنال آنالوگ ۲۰-۴ میلی‌آمپر بهره می‌برد.

اتصالات ضروری و اختیاری

در پروتکل HART، اتصالات ضروری شامل دو سیم برای سیگنال ۲۰-۴ میلی‌آمپر است که هم برای تأمین برق و هم برای انتقال سیگنال استفاده می‌شود. این دو سیم به ترتیب به دستگاه اندازه‌گیری (مانند ترانسمیتر) و سیستم کنترل یا نمایشگر متصل می‌شوند.

اتصالات اختیاری ممکن است شامل یک مقاومت ۲۵۰ اهمی در مسیر سیگنال باشد که برای تبدیل سیگنال جریان به ولتاژ جهت مانیتورینگ یا اتصال به دستگاه‌های دیگر استفاده می‌شود.

(۳)

ارتباط در پروتکل HART : سریال یا موازی؟

پروتکل HART یک پروتکل سریال است. این پروتکل از روش FSK (Frequency Shift Keying) برای ارسال داده‌های دیجیتال روی سیگنال آنالوگ ۴-۲۰ میلی آمپر استفاده می‌کند. ارتباط سریال به این معنی است که داده‌ها بیت به بیت و به صورت متوالی ارسال می‌شوند، نه به صورت همزمان روی چندین خط (موازی).

نوع انکودینگ در پروتکل HART

پروتکل HART از مدولاسیون FSK بر اساس استاندارد Bell 202 استفاده می‌کند. در این روش، داده‌های دیجیتال با دو فرکانس متفاوت کدگذاری می‌شوند:

✓ ۱۲۰۰ هرتز → نمایش بیت '۱'

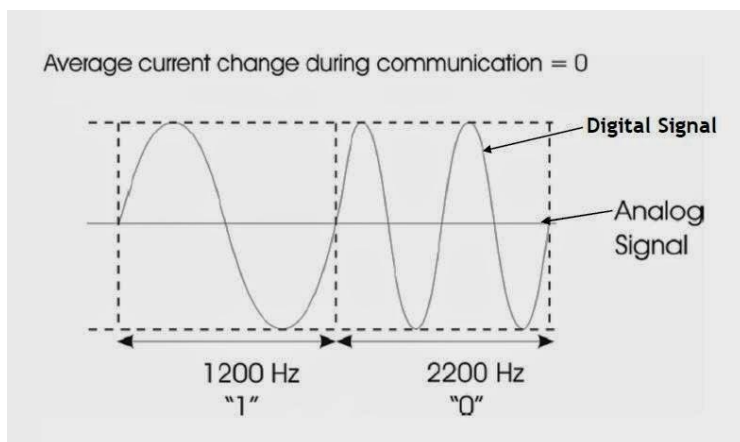
✓ ۲۲۰۰ هرتز → نمایش بیت '۰'

این نوع انکودینگ باعث می‌شود که سیگنال دیجیتال بدون اختلال روی سیگنال آنالوگ ۴-۲۰ میلی آمپر قرار گیرد.

نحوه تولید سیگنال در پروتکل HART

سیگنال در HART با تولید و ترکیب دو فرکانس ۱۲۰۰ Hz و ۲۲۰۰ Hz انجام می‌شود. این فرکانس‌ها بر روی سیگنال جریان DC ۴-۲۰ میلی آمپر به صورت متناوب اضافه می‌شوند، اما دامنه آن‌ها کم است (معمولاً در حدود ± 0.5 میلی آمپر) تا تأثیری بر اندازه‌گیری‌های آنالوگ نداشته باشد.

مدارهای تولید سیگنال معمولاً شامل یک مدولاتور FSK هستند که فرکانس مناسب را بر اساس داده‌های ارسال شده تولید می‌کند و آن را به سیگنال ۴-۲۰ میلی آمپر اضافه می‌نماید.



روش انتقال: همزمان یا ناهمزمان؟

پروتکل HART از روش انتقال ناهمزمان (Asynchronous Transmission) استفاده می‌کند. در این روش:

- ◆ داده‌ها در فریم‌های مجزا ارسال می‌شوند.
 - ◆ هر فریم دارای بیت‌های شروع و توقف است.
 - ◆ نیازی به هماهنگی (Clock Signal) بین فرستنده و گیرنده وجود ندارد.
- این ویژگی باعث می‌شود که ارتباط بین دستگاه‌ها بدون نیاز به همزمان‌سازی پیچیده قابل اجرا باشد، که برای سیستم‌های صنعتی پراکنده و طولانی‌مدت بسیار مناسب است.

(۴)

اتصال چندین دستگاه در پروتکل HART : امکان‌پذیر است؟

بله، پروتکل HART قابلیت اتصال چندین دستگاه را دارد، اما روش اتصال آن به نوع شبکه HART بستگی دارد. این پروتکل می‌تواند در دو حالت (Point-to-Point نقطه‌به‌نقطه) و (Multidrop چندقطبی) عمل کند.

۱. روش اتصال نقطه‌به‌نقطه (Point-to-Point)

- ◆ این روش رایج‌ترین روش اتصال در HART است.
- ◆ هر دستگاه HART (مثلاً یک ترانسمیتر) مستقیماً به یک کنترلر (DCS، PLC یا HART Communicator) متصل می‌شود.
- ◆ سیگنال ۲۰-۴ میلی‌آمپر همچنان برای ارسال مقدار اندازه‌گیری شده استفاده می‌شود، و داده‌های دیجیتال از طریق مدولاسیون FSK روی آن ارسال می‌شوند.
- ◆ این روش فقط امکان اتصال دو دستگاه (یک کنترلر و یک دستگاه) را دارد.

۲. روش اتصال چندقطبی (Multidrop)

- ◆ در این روش، چندین دستگاه HART به یک خط ارتباطی مشترک متصل می‌شوند.
- ◆ همه دستگاه‌ها به طور موازی روی دو سیم مشترک قرار می‌گیرند.

◆ مقدار جریان هر دستگاه روی مقدار ثابت ۴ میلی آمپر قفل می شود (بنابراین سیگنال آنالوگ قابل استفاده نیست).

◆ ارتباط فقط از طریق داده های دیجیتال انجام می شود.

◆ حداکثر ۱۵ دستگاه را می توان به یک خط متصل کرد.

✓ کاربرد روش Multidrop: این روش بیشتر برای نظارت و کالیبراسیون استفاده می شود، زیرا سیگنال آنالوگ دیگر برای کنترل فرایند در دسترس نیست.

چالش مدیریت برخورد در پروتکل HART

◆ در ارتباطات چندقطبی (Multidrop)، چندین دستگاه می توانند همزمان تلاش کنند داده ارسال کنند، که باعث برخورد در سیگنال ها می شود.

◆ برای جلوگیری از این مشکل، پروتکل HART از روش Master-Slave استفاده می کند:

- یک Master (کنترل کننده) درخواست ارسال داده می کند.
- دستگاه ها (Slaves) فقط در پاسخ به این درخواست داده ارسال می کنند.
- هیچ دستگاهی بدون اجازه Master داده ارسال نمی کند.

✓ نتیجه: این روش از برخورد داده ها جلوگیری کرده و ارتباط را هماهنگ می کند.

چرا HART برای اتصال چندین دستگاه در حالت عادی طراحی نشده است؟

◆ HART بر اساس سیگنال ۴-۲۰ میلی آمپر طراحی شده که به طور ذاتی برای کنترل یک دستگاه در هر حلقه بهینه شده است.

◆ در حالت استاندارد، سیگنال آنالوگ مقدار تنها یک متغیر فرآیندی (مثلاً دما یا فشار) را می تواند ارسال کند، بنابراین کنترل چند دستگاه با این سیگنال عملی نیست.

◆ برای ارتباط چند دستگاه به طور مؤثر، پروتکل های کاملاً دیجیتال مانند Modbus یا Profibus مناسب تر هستند.

۱. آیا پروتکل HART آدرس دهی دارد؟

✓ بله، پروتکل HART از آدرس دهی ساده‌ای برای شناسایی دستگاه‌ها استفاده می‌کند، اما مسیریابی (Routing) ندارد.

۲. نحوه آدرس دهی در HART

◆ در حالت نقطه به نقطه (Point-to-Point)، تنها یک دستگاه متصل است، بنابراین آدرس دهی پیچیده‌ای نیاز نیست.

◆ در حالت چند قطبی (Multidrop)، هر دستگاه یک آدرس منحصر به فرد (Polling Address) بین ۰ تا ۱۵ دارد.

◆ فرمت آدرس در HART شامل دو نوع است:

- آدرس کوتاه: (Short Frame Addressing) فقط از بیت‌های کم (۴ بیت) برای آدرس دهی استفاده می‌کند.
- آدرس طولانی: (Long Frame Addressing) از بیت‌های بیشتری (۳۸ بیت) برای آدرس دهی دقیق‌تر بهره می‌برد.

✓ در حالت Multidrop، کنترلر (Master) با ارسال آدرس دستگاه مشخص، داده را از آن درخواست می‌کند.

۳. آیا پروتکل HART مسیریابی (Routing) دارد؟

✗ خیر، پروتکل HART مسیریابی ندارد.

۴. چرا HART نیازی به مسیریابی ندارد؟

۱. ساختار ساده شبکه

- پروتکل HART به طور معمول در شبکه‌های کوچک و مستقیم (مثل یک خط ارتباطی با چند دستگاه) استفاده می‌شود.

- نیازی به ارسال داده بین گره‌های مختلف از طریق مسیرهای پیچیده وجود ندارد.
- ۲. روش ارتباط Master-Slave
 - همیشه یک کنترلر (Master) با دستگاه‌های زیرمجموعه (Slaves) مستقیماً ارتباط دارد.
 - برخلاف شبکه‌های پیچیده که در آن‌ها نیاز به ارسال داده بین چند گره وجود دارد، در HART هر دستگاه فقط مستقیماً به Master پاسخ می‌دهد.
- ۳. عدم نیاز به تغییر مسیر داده
 - هر دستگاه مستقیماً روی یک خط دو سیمه متصل است، بنابراین مسیریابی داده‌ها از طریق چندین نود لازم نیست.
- ۴. کاربرد در سیستم‌های صنعتی سنتی
 - HART برای جایگزینی ارتباط آنالوگ ۴-۲۰ میلی‌آمپر طراحی شده است، که ذاتاً ساختاری نقطه‌به‌نقطه دارد.

(۶)

مدیریت جریان داده چیست؟

مدیریت جریان داده (Flow Control) روشی است که برای کنترل سرعت انتقال داده بین فرستنده و گیرنده استفاده می‌شود. این کار باعث جلوگیری از ازدحام (Congestion) و از بین رفتن داده‌ها در صورت تفاوت سرعت پردازش فرستنده و گیرنده می‌شود.

روش‌های رایج مدیریت جریان داده شامل:

۱. کنترل مبتنی بر توقف و انتظار (Stop-and-Wait) – فرستنده پس از ارسال هر بسته، منتظر تأیید گیرنده می‌ماند.
۲. کنترل مبتنی بر پنجره لغزان (Sliding Window) – فرستنده می‌تواند چندین بسته را قبل از دریافت تأیید ارسال کند.
۳. کنترل مبتنی بر نرم‌افزار (XON/XOFF) و سخت‌افزار (RTS/CTS) – استفاده از سیگنال‌های کنترلی برای مدیریت ارسال داده.

مدیریت جریان داده در پروتکل HART

✓ پروتکل HART نیازی به مدیریت جریان داده پیچیده ندارد، زیرا از روش ارتباط Master-Slave استفاده می‌کند.

نحوه پیاده‌سازی در HART :

۱. ارتباط به صورت درخواست و پاسخ (Request-Response) انجام می‌شود:
 - Master (کنترل‌کننده) یک درخواست (Command Message) به دستگاه ارسال می‌کند.
 - دستگاه Slave فقط در پاسخ به درخواست Master داده را ارسال می‌کند.
 - این روش باعث می‌شود که فرستنده و گیرنده همیشه همگام باشند و داده اضافی ارسال نشود.
۲. عدم نیاز به مدیریت پیچیده جریان:
 - چون در هر لحظه فقط یک دستگاه می‌تواند داده ارسال کند، نیازی به مدیریت ازدحام و سرعت انتقال نیست.
 - کنترل‌کننده می‌تواند نرخ ارسال داده را با تنظیم نرخ Polling (نرخ درخواست داده از دستگاه‌ها) کنترل کند.
۳. عدم استفاده از روش‌های Sliding Window یا XON/XOFF:
 - چون ارتباط HART ناهمزمان و مبتنی بر پیام است، نیازی به کنترل نرم‌افزاری یا سخت‌افزاری جریان داده ندارد.
 - دستگاه Slave فقط در صورت دریافت درخواست، داده را ارسال می‌کند، بنابراین هیچ داده‌ای در مسیر ذخیره یا منتظر پردازش نمی‌ماند.

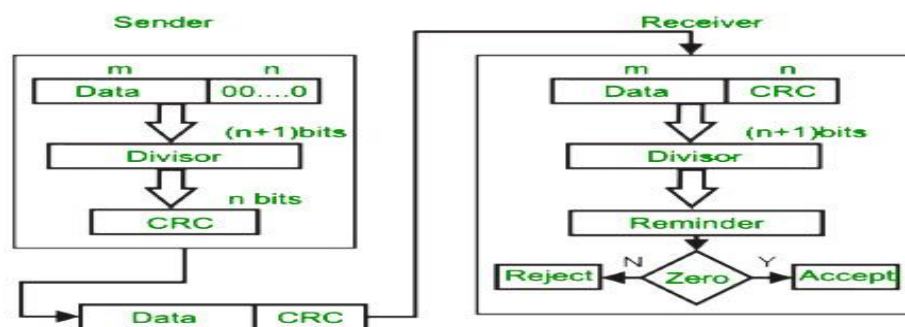
(۷)

تشخیص خطا در لایه‌های مختلف مدل OSI به روش‌ها و مکانیزم‌های متفاوتی بستگی دارد که بسته به نوع داده‌ها و چالش‌های موجود در هر لایه متفاوت است. در ادامه، نحوه تشخیص خطا در هر یک از لایه‌های مدل OSI توضیح داده می‌شود:

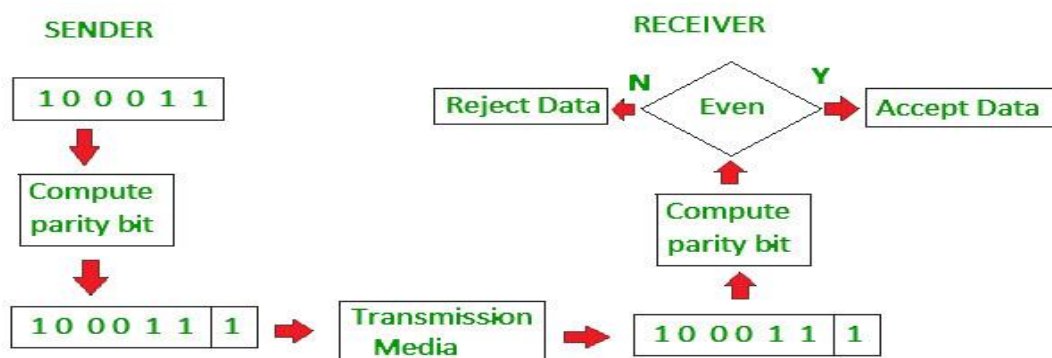
۱. لایه فیزیکی (Physical Layer)

این لایه مسئول انتقال داده‌ها به صورت سیگنال‌های الکتریکی یا نوری است و خطاها عمدتاً به دلیل نویز، تداخل و مشکلات فیزیکی در رسانه انتقال به وجود می‌آیند. روش‌های تشخیص خطا در این لایه شامل:

- تشخیص خطای CRC: در این روش، یک دنباله بیتی اضافی به داده‌ها اضافه می‌شود تا گیرنده بتواند صحت داده‌ها را بررسی کند. این تکنیک معمولاً در ارتباطات شبکه‌ای استفاده می‌شود.



- بررسی توازن: در این روش، تعداد بیت‌های ۱ در یک فریم شمارش می‌شود و اگر تعداد آنها درست نباشد، خطا تشخیص داده می‌شود.



- تشخیص بازگشت به صفر: در این روش، تغییرات ناگهانی در سطح سیگنال (سیگنال‌های دیجیتالی) می‌تواند به عنوان نشانه‌ای از وقوع خطا شناسایی شود.

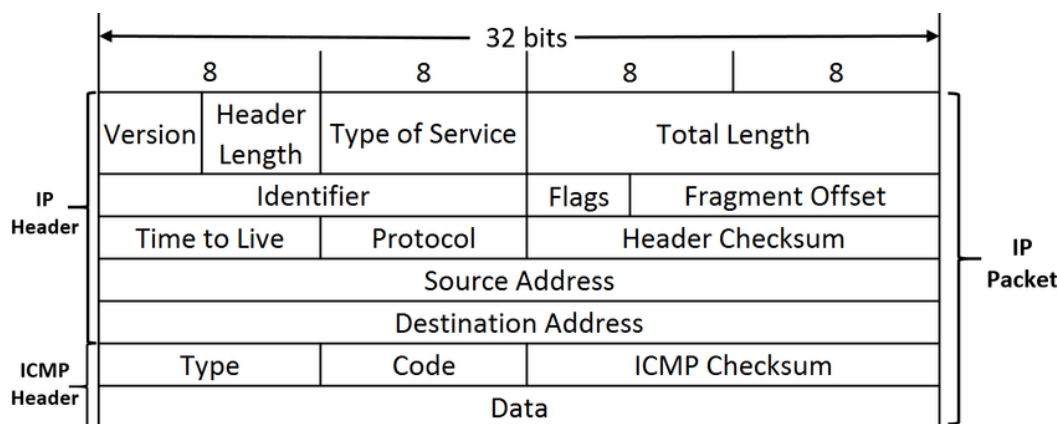
۲. لایه داده (Data Link Layer)

این لایه مسئول بسته‌بندی داده‌ها در فریم‌ها است و خطاها معمولاً ناشی از مشکلات فریم‌سازی و همگام‌سازی می‌باشند. روش‌های تشخیص خطا در این لایه شامل:

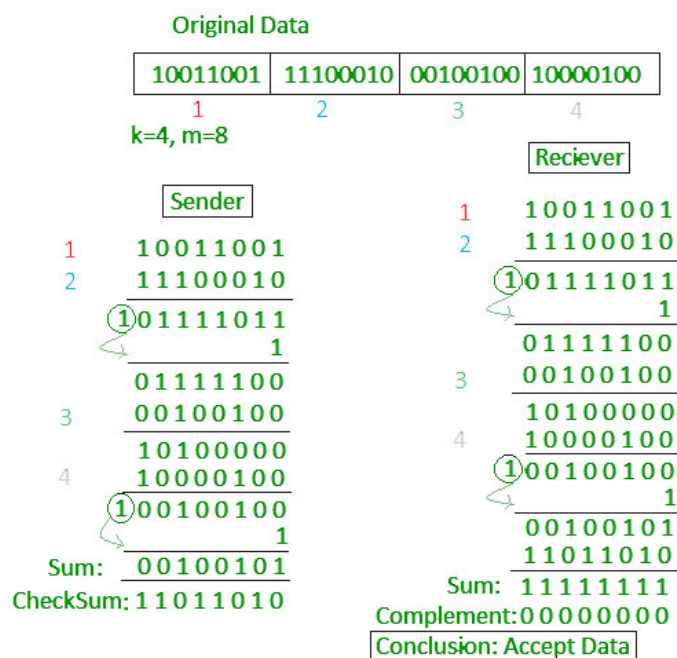
- ## Automatic Repeat Request(ARQ)



- ICMP (Internet Control Message Protocol): پیام‌های ICMP مانند Echo Request و Destination Unreachable برای تشخیص مشکلات مسیریابی و وضعیت مقصد استفاده می‌شوند.

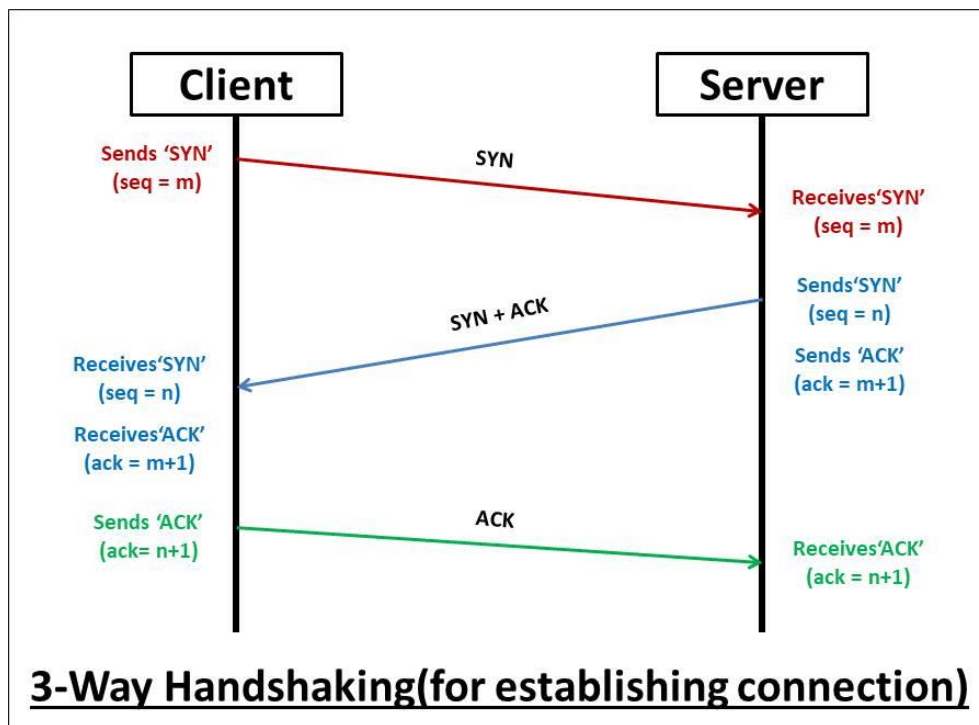


- Checksum: در سرآیند IP ، از Checksum برای بررسی صحت داده‌ها و تشخیص خطاها استفاده می‌شود.



۴. لایه انتقال (Transport Layer)

- در این لایه، خطاها معمولاً به دلیل از دست رفتن بسته‌ها، ترتیب اشتباه بسته‌ها یا خطاهای لایه‌های پایین‌تر ایجاد می‌شوند. روش‌های تشخیص خطا در این لایه شامل:
- شماره دنباله: مشابه لایه داده، از شماره دنباله برای شناسایی بسته‌های گم‌شده یا تکراری استفاده می‌شود.
 - ACK (Acknowledgment): گیرنده پس از دریافت بسته، با ارسال ACK تأیید می‌کند که بسته را دریافت کرده است. اگر فرستنده ACK دریافت نکند، بسته مجدداً ارسال می‌شود.



- تایمرهای بازارسال: اگر فرستنده تایمر خود را برای دریافت ACK به پایان رساند و هیچ ACK دریافت نکرد، بسته را مجدداً ارسال می کند.

۵. لایه جلسه (Session Layer)

در این لایه، خطاها معمولاً ناشی از قطع ارتباط یا مشکلات همگام سازی می باشند. روش های تشخیص خطا در این لایه شامل:

- چک پوینت ها: اطلاعات مهم در فواصل زمانی معین ذخیره می شود تا در صورت بروز خطا، ارتباط از آخرین چک پوینت بازیابی شود.
- تایمرهای نظارت بر زمان: اگر ارتباط برای مدت زمان مشخصی قطع شود، خطا تشخیص داده می شود.

۶. لایه ارائه (Presentation Layer)

در این لایه، خطاها معمولاً به دلیل مشکلات در رمزگذاری یا فشرده سازی داده ها رخ می دهند. روش های تشخیص خطا در این لایه شامل:

- CRC: برای تشخیص خطا در داده های رمزگذاری شده یا فشرده شده استفاده می شود.

- چک‌های یکپارچگی: این روش برای بررسی صحت داده‌های رمزگذاری‌شده یا فشرده‌شده به کار می‌رود.

۷. لایه کاربرد (Application Layer)

در این لایه، خطاها بیشتر به دلیل مشکلات در پروتکل‌های کاربردی مانند HTTP، FTP یا SMTP ایجاد می‌شوند. روش‌های تشخیص خطا در این لایه شامل:

- کدهای وضعیت HTTP: برای نشان دادن موفقیت یا شکست یک درخواست، از کدهای وضعیت مانند ۴۰۴ (Not Found) یا ۵۰۰ (Internal Server Error) استفاده می‌شود.
- پیام‌های خطا: پروتکل‌های کاربردی معمولاً پیام‌های خطا ارسال می‌کنند تا مشکلات را به کاربر یا سیستم مقصد گزارش دهند.

جمع‌بندی:

تشخیص خطا در مدل OSI یک فرآیند چندلایه است که از هر لایه برای شناسایی خطاها استفاده می‌شود. این مکانیزم‌ها از ساده‌ترین روش‌ها مانند CRC در لایه فیزیکی و داده، تا پیچیده‌ترین روش‌ها مانند تایمرها و ACK در لایه‌های بالاتر، در هر لایه برای تشخیص و تصحیح خطاها به کار می‌روند.

(۸)

تصحیح خطا در پروتکل HART

پروتکل HART از تشخیص خطا (Error Detection) استفاده می‌کند، اما تصحیح خطا (Error Correction) به معنای ارسال مجدد داده‌ها انجام می‌شود و مکانیسمی برای اصلاح خودکار داده‌های خراب ندارد.

روش‌های تشخیص خطا در HART

HART از دو روش اصلی برای تشخیص خطا در پیام‌های ارسال‌شده استفاده می‌کند:

۱. استفاده از Checksum (بررسی مجموع)

- ✓ هر پیام HART شامل یک فیلد Checksum (مجموع بررسی) در انتهای فریم است.
- ✓ این مقدار حاصل عملیات XOR روی بایت‌های پیام است.
- ✓ گیرنده پس از دریافت پیام، مقدار Checksum را محاسبه و بررسی می‌کند که آیا مطابق مقدار دریافتی است یا نه.
- ✓ اگر مقدار محاسبه‌شده با مقدار دریافت‌شده مطابقت نداشته باشد، پیام دارای خطا است و باید دوباره ارسال شود.

۲. بررسی فریم و تاییدیه پیام (Message Acknowledgment)

- ✓ پس از دریافت هر پیام، گیرنده یک پیام تأییدیه (ACK) یا خطا (NAK) به فرستنده ارسال می‌کند.
- ✓ اگر پیام دارای خطا باشد، گیرنده یک NAK (Negative Acknowledgment) ارسال کرده و فرستنده باید پیام را مجدداً بفرستد.
- ✓ اگر پیام صحیح باشد، (ACK (Acknowledgment ارسال شده و ارتباط ادامه پیدا می‌کند.

محدودیت‌های تصحیح خطا در HART

- ✗ HART مکانیسم پیچیده‌ای برای تصحیح خودکار خطا (مانند کدهای تصحیح خطا در برخی پروتکل‌های مدرن) ندارد.
- ✗ در صورت بروز خطا، پیام باید مجدداً ارسال شود.
- ✗ از آنجا که HART برای سیستم‌های صنعتی حساس طراحی شده است، این روش ساده اما مؤثر تشخیص خطا باعث افزایش قابلیت اطمینان ارتباط می‌شود.

(۹)

انواع پیام‌ها در پروتکل HART

در پروتکل HART، پیام‌ها به دو دسته کلی تقسیم می‌شوند:

۱. پیام‌های درخواست (Request Messages) → ارسال‌شده از Master به Slave
۲. پیام‌های پاسخ (Response Messages) → ارسال‌شده از Slave به Master

بر اساس عملکرد، پیام‌های HART شامل موارد زیر هستند:

- ✓ پیام‌های فرمان (Command Messages): شامل دستورات کنترلی از Master به Slave
- ✓ پیام‌های داده‌ای (Data Messages): شامل اطلاعات اندازه‌گیری شده یا تنظیمات دستگاه
- ✓ پیام‌های تأیید (Acknowledgment Messages - ACK/NAK): برای تأیید یا رد درخواست‌ها
- ✓ پیام‌های خطا (Error Messages): در صورت وجود مشکل در ارتباط ارسال می‌شوند

فرمت پیام در پروتکل HART

هر پیام HART دارای یک قالب استاندارد است که شامل فیلدهای زیر می‌شود:

بخش پیام	توضیح
Preamble (مقدمه)	چندین بایت برای همگام‌سازی ارتباط (حداقل ۵ و حداکثر ۲۰ بایت 0xFF)
Start Byte (بایت شروع)	مشخص‌کننده نوع پیام (پیام Master یا Slave)
Address (آدرس دستگاه)	آدرس دستگاه گیرنده در حالت Multidrop
Command (فرمان)	نوع دستور (خواندن، نوشتن، پیکربندی و ...)
Byte Count (تعداد بایت‌های داده)	تعداد بایت‌های داده موجود در پیام
Data (داده‌ها)	اطلاعات اندازه‌گیری شده یا پارامترهای تنظیمی
Checksum (بررسی صحت)	مقدار XOR از تمام بایت‌های پیام برای تشخیص خطا

۱. فرمت پیام درخواست (Request Message - Master to Slave)

ساختار پیام درخواست از Master به Slave :

| Preamble | Start | Address | Command | Byte Count | Data |
Checksum

✓ توضیحات:

- Master با ارسال یک دستور از دستگاه Slave درخواست داده می‌کند.
- فیلد Command مشخص می‌کند که چه عملی باید انجام شود (مثلاً خواندن مقدار فشار، تغییر پارامتر، کالیبراسیون، و ...).

۲. فرمت پیام پاسخ (Response Message - Slave to Master)

ساختار پیام پاسخ از Slave به Master :

| Preamble | Start | Address | Status | Byte Count | Data | Checksum |

✓ توضیحات:

- Slave در پاسخ به درخواست Master، مقدار خوانده‌شده یا تأییدیه ارسال می‌کند.
- فیلد Status مشخص می‌کند که درخواست موفقیت‌آمیز بوده است یا خطایی رخ داده است.

۳. فرمت پیام تأیید یا خطا (ACK/NAK Message)

ساختار پیام تأیید (ACK) یا رد (NAK) :

| Preamble | Start | Address | Status | Byte Count | Error Code |
Checksum

✓ توضیحات:

- اگر پیام درخواست بدون خطا پردازش شود، پیام ACK (Acknowledgment) ارسال می‌شود.
 - اگر خطایی رخ دهد، پیام NAK (Negative Acknowledgment) شامل یک Error Code ارسال می‌شود.
-