POWERLINK 的功能和特点

王谨秋

POWERLINK 开发板，POWERLINK 协议软件和技术支持，IO 模块，运动控制器，工业机器人控制器。

QQ 群： 151181908
联系人： 王先生
手机：13917489045（微信同号）
邮箱：openpowerlink@163.com
网址： http://www.openat.cn

第三章 POWERLINK 的功能和特点.....3
3.1 应用案例.....3
3.2 一“网”到底.....3
3.2.1 多路复用.....4
3.2.2 大数据量通信.....5
3.2.3 诊断.....5
3.2.4 网络配置.....6
3.2.5 实现方案.....6
3.2.6 开发难度.....6
3.3 性能参数.....7
3.4 网络拓扑.....8
3.4.1 网络拓扑.....8
3.4.2 节点的寻址.....8
3.5 热插拔.....8
3.6 冗余.....9
3.6.1 双网冗余.....9
3.6.2 环形冗余.....15
3.6.3 多主冗余.....26
3.6.4 冗余系统的典型拓扑结构.....38
3.7 交叉通信.....40
3.8 实时域与非实时域.....40
3.9 基于 POWERLINK 的功能安全.....41
3.9.1 适用于所有现场总线.....41
3.9.2openSAFETY 原理.....42

第三章 POWERLINK 的功能和特点

POWERLINK 所具有功能以及特点决定了他的用途. POWERLINK 的最短周期可以达到几十微秒,最长可到几十秒。支持各种冗余技术，支持周期性通信以及非周期性通信。这些特点决定了 POWERLINK 可以满足工业上的各种需求。典型的应用主要是运动控制和过程控制,以及工厂自动化。下面介绍几个主要的应用案例。

3.1 应用案例

POWERLINK 技术应用广泛，在运动控制和过程控制上面都有众多国内外知名厂家支持：

- 运动控制

典型应用: 伺服驱动器的控制，用于各种机器系统，如包装机，纺织机，印刷机，机器人等。

典型厂家：B&R，ABB，武汉迈信电气技术有限公司，上海新时达电气股份有限公司等

- 过程控制

典型应用 ：DCS 系统，工厂自动化

典型厂家 ：Alstom，B&R，北京和利时集团，北京四方继保自动化股份有限公司，南京南瑞，南京大全电气有限公司，中国南车，卡斯柯信号有限公司等

3.2 一“网”到底

POWERLINK 物理层采用普通以太网的物理层，因此可以使用工厂中现有的以太网布线，从机器设备的基本单元，到整台设备，到生产线，再到办公室都可以使用以太网，从而实现一 “网”到底，如图 3-1 所示。

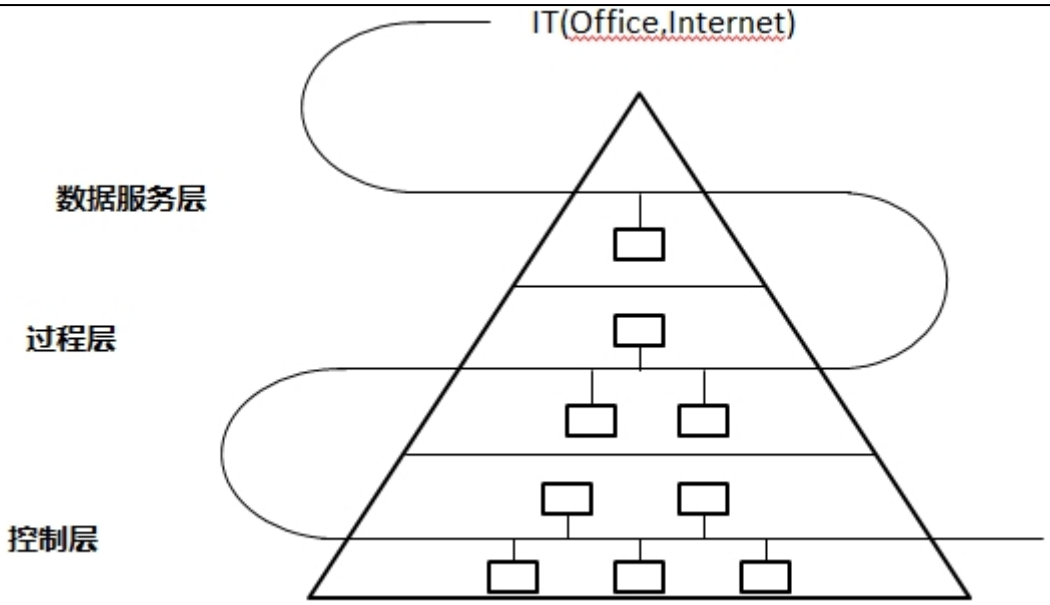

图 3-1 一“网”到“底”模型

3.2.1 多路复用

网络中不同的节点具有不同的通讯周期， 兼顾快速设备和慢速设备，使网络配置达到最优。

同步通信与异步通信：

一个 POWERLINK 周期既包含同步通信阶段，也包括异步通信阶段。同步通信阶段即周期性通信，用于周期性传输通信数据； 异步通信即非周期性通信，用于传输非周期性的数据。

因此 POWERLINK 网络可以适用于各种设备。如图 3-2 所示：

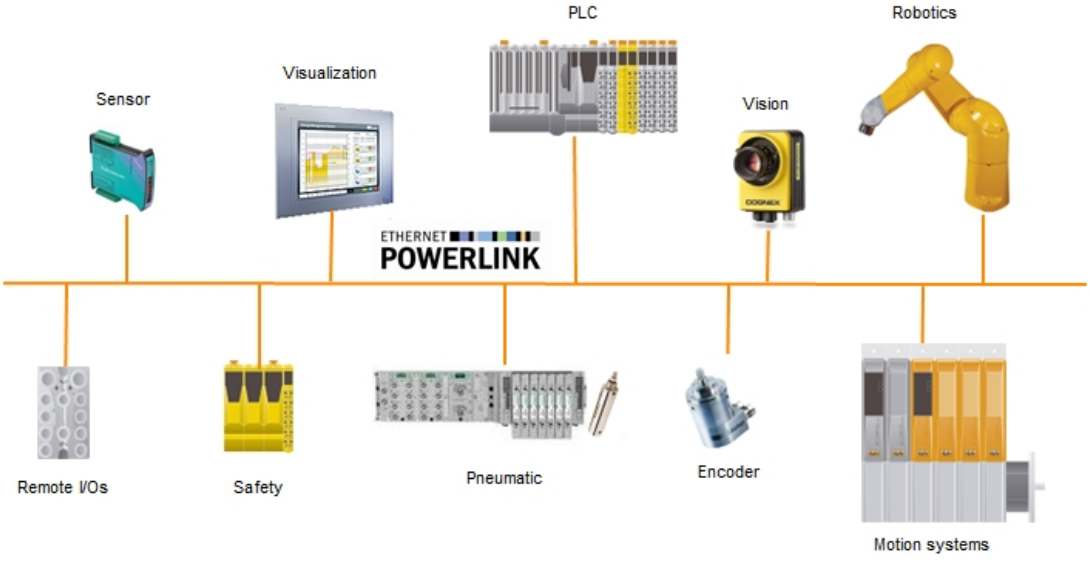

图 3-2 POWERLINK 网络系统

3.2.2 大数据量通信

POWERLINK 的每个节点的发送和接收，分别采用独立的数据帧，每个数据帧最大为 1490Bytes 。一些采用集束帧的协议相比，通信量提高数百倍。在“束帧协议”里，网络中所有节点的发送和接收共用一个数据帧,这种机制无法满足大数据量传输的场合。

在过程控制中，网络的节点数多，每个节点传输的数据量大，因而 POWERLINK 很受欢迎。

3.2.3 诊断

组建一个网络，网络启动后，可能网络中的某些节点配置错误，或者节点号冲突等，导致网络异常。需要有手段，来诊断网络的通信状况， 找出故障的原因和故障点，从而修理网络异常。

POWERLINK 的诊断有两种工具：Wireshark 和 Omnipeak。

诊断的方法是在将诊断的计算机接入到 POWERLINK 网络中，Wireshark 或 Omnipeak 自动抓取通信数据包，分析并诊断网络的通信状况，以及时序。这种诊断不占用任何带宽，而且是标准的以太网诊断工具，只需要一台带有以太网接口的 PC。

3.2.4 网络配置

POWERLINK 使用开源的网络配置工具 -- openCONFIGURATOR， 用户可以单独使用该工具，也可以将该工具的代码集成到自己的软件中，成为自己软件的一部分。

使用该软件，可以方便的组建，配置 POWERLINK 网络

3.2.5 实现方案

POWERLINK 具有以下解决方案：

- POWERLINK 纯软件解决方案
  - 独立于平台的解决方案
  - 任意操作系统：VxWorks, Linux,Windows,WinCE
  - 任意处理器：ARM , DSP ,X86 等
  - 任意的网卡
  - 遵循 Open Source License (BSD)开源协议
  - www.sourceforge.net/projects/openPOWERLINK
- FPGA 解决方案
  - 高性能
  - 超短的循环周期：T = 35 + N*15 us (N 为从站的个数)

3.2.6 开发难度

- 零开发风险
  - 无需开发工作，只需学会如何使用

- 极短的产品开发周期
- 集成 POWERLINK 软件只需几个小时

▪ 100%的互联互通

- 集成标准的 CANopen 代码，保证各个厂家的 POWERLINK 设备互联互通
- 现成的开源组态工具
- 方便灵活的配置网络

3.3 性能参数

（1） 循环周期

100us（高性能 CPU 或者 FPGA 的 VHDL 解决方案）

200us（低性能 CPU 或者 FPGA 的软核解决方案)

循环周期的定义是指网络上所有的设备都通信一次，即网络上所有的设备都 Preq/Pres 一次，所花费的时间。循环周期的长短取决于三个因素：1.节点数、2.每个节点传输的数据量、3.传输速度（波特率）。

（2） 抖动<<1us

抖动的定义是指实际循环周期中最大值与最小值的差。例如你设定的循环周期是 200us，但是实际的循环周期不可能是非常准确的 200us，有可能是 199.999us，也有可能是 200.0001us，假如最大循环周期为 200.5us，最小循环周期为 199.5us，循环周期会在 199.5-200.5 之间抖动。抖动的大小和运行 POWERLINK 硬件/软件平台有关，如果采用 Windows 操作系统在没有实时扩展的情况下，抖动可能在毫秒级；如果使用 FPGA，抖动小于 100 纳秒。

（3） 网络容量

支持 240 个节点，每个节点支持 1500Bytes 的输入和 1500Bytes 的输出。

240 个节点意味着在一个 POWERLINK 的网络中可以连接 240 个设备或者 I/O 站，每个设备或 I/O 站每个循环周期 1500Bytes 的输入和 1500Bytes 的输出，所以网络容量为 240*（1500+1500）=720，000Bytes。

（4） 物理层速度

POWERLINK 物理层采用普通以太网物理层，支持的速率为 100Mbps，

1000Mbps，10000Mbps.

3.4 网络拓扑

3.4.1 网络拓扑

由于 POWERLINK 的物理层采用标准的以太网，因此以太网支持的所有拓扑结构他都支持。而且可以使用 HUB 和 SWITCH 等标准的网络设备，这使的用户组网非常灵活，如：

- 菊花链形
- 树形
- 星形
- 环形
- 以及任意组合

因为逻辑与物理无关，用户在编写程序的时候，无需考虑拓扑结构。网络中的每个节点都有一个节点号，POWERLINK 是通过节点号来寻址节点，而不是通过节点的物理位置来寻址，因此逻辑与物理无关。

由于协议独立的拓扑配置功能，POWERLINK 的网络拓扑与机器的功能无关。因此 POWERLINK 的用户无需考虑任何网络相关的需求，只需专注满足设备制造的需求。POWERLINK 环境里的控制器不需要必须了解网络更底层的内容。

3.4.2 节点的寻址

POWERLINKMAC 的寻址依照 IEEE802.3。每个设备的地址都是唯一的，我们称之为节点 ID。因此新增一个设备，也就意味着引入一个新地址。节点 ID 可以通过设备上的拨码开关手动设置。也可以通过软件设置：拨码拨到 FF，这就默认为软件配置地址。此外还有第三个可选方法，POWERLINK 也可支持标准 IP 地址。因此，POWERLINK 设备可以通过万维网，随时随地被寻址（需要通过路由或网关）。

3.5 热插拔

热插拔意味着从正在运行的网络上拔除或插入设备；系统会自动意识到网络的变化。POWERLINK 支持热插拔，而且不会影响整个网络的实时性。根据这个属性，可以实现网络的动态配置，即可以动态的增加，减少网络中的节点。

实时总线上，热插拔能力带给用户两个重要的好处：当模块增加或替换时，无需重新配置；在运行的网络中替换或激活一个新模块不会导致网络瘫痪。系统会继续工作，不管是不断的扩展或者本地的替换，其实时能力不受影响。某些场合，系统不能断电，这就造成了如果不支持热插拔，即使小机器一部分被替换，都会不可避免地导致系统停机。

配置管理是 POWERLINK 系统最重要的一部分。它能本地保存自己和系统中所有其他设备的配置数据，并在系统启动时加载它们。这个特性可以实现即插即用，这使得初始安装和设备替换非常简单。

POWERLINK 允许无限制的即插即用，因为该系统集成了 CANopen 机制。新设备只需插入，就可立即工作。

3.6 冗余

POWERLINK 的冗余包括三种冗余：双网冗余，环网冗余和多主冗余。

3.6.1 双网冗余

双网冗余顾名思义，就是系统中有两个独立的网络，当一个网络出现故障，另一个网络依然可以工作。双网冗余是一种物理介质的冗余,又称 “线缆冗余”，对于每个节点，都有两个网络接口，或多个网络接口。

3.6.1.1 双网冗余的机制

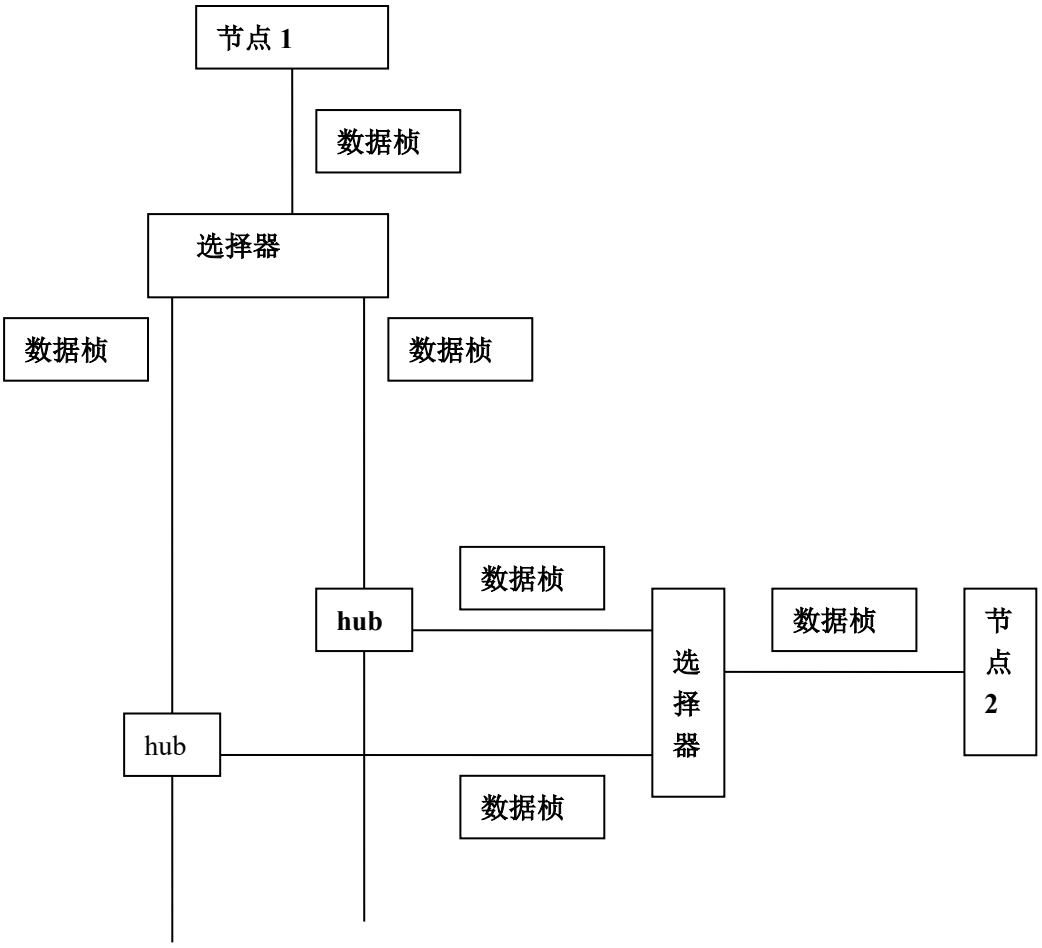

图 3-3 线缆冗余模型

图 3-3 所示，节点 1 和节点 2 既可以是主站节点也可以从站节点。节点 1 发出的数据帧在经过选择器的时候，一个数据帧被复制成两个数据帧，同时在两个网络中传输。在接收方节点 2 的选择器处，会同时有两个数据帧到来，选择器选择其中一个，发给节点 2。同理，当节点 2 发送数据时，在经过节点 2 的选择器时，也被复制成成两个数据帧，同时在两个网络中传输。在接收方节点 1 的选择器处，会同时有两个数据帧到来，选择器选择其中一个，发给节点 1。

这样，两个网络同时工作，当一个网络出现故障，网络节点可以从另外一个网络收发数据。这种机制的好处是无需网络切换，所以当一个网络出现故障时，不会影响另外

一个网络的运行，整个系统的通信没有延迟，不会丢失数据帧。

3.6.1.2 线路状态

当某个网段出现线路故障时，需要将此信息通知应用程序，以帮助用户修理网络。选择器检查网络状态的方法如下：

1. 选择器检查每个网络数据接收情况，假设某个选择器有两个网口，一个称为 A 网，另一个称为 B 网。如果 B 网已经接收到数据，而 A 网从 B 网接收到数据时开始，在一段时间 T 内没有收到任何数据（或者在一定时间内 B 网已经收到了多于 2 次数据帧，而 A 网在这段时间内没有收到数据），就说明 A 网出现了故障。也可以简单的检查节点的网口状态，即网口的 Link 状态和 Active 状态的信号。
2. 当选择器检测到某个网络出现故障时，将该信息上报给与其连的 POWERLINK 节点，该 POWERLINK 节点的协议栈需要将这个信息上报给网络中的其它节点，对于从站节点，需要将该信息包含在 PollResponse, StatusResponse, IdentResponse 这三种上报的数据帧里；对于主站节点，需要将该信息包含在 PollReques 数据帧里发给相应的从站。
3. 网路信息在 PollResponse, StatusResponse, IdentResponse，PollReques 数据帧中的“FLS”,“SLS”。FLS 是英文“First link status”的缩写，SLS 是英文“Second link status”的缩写，其在数据帧中位置如图 3-4：

	Bit Offset							
Octet Offset	7	6	5	4	3	2	1	0
0	Res	Massage Type						
1	Destination							
2	source							
3	xxx							
4	xx	xx	xx	xx	xx	xx	xx	xx
5	FLS	SLS	PR			RS		
6-n	xxx							

图 3-4 线缆状态字段在数据帧中的位置

在 POWERLINK 数据帧的第 5 个字节的第 6 和第 7 比特位分别表示第一个网络的状态(FLS)和第二个网络的网络的状态(SLS)：

Bit 7 = First Link Status (FLS)　(0 = Link OK, 1 = Link not OK).

Bit 6 = Second Link Status (SLS)　(0 = Link OK, 1 = Link not OK)

注意: POWERLINK 数据帧的第 5 个 BYTE,是以太网数据帧的第 19 个 BYTE。

3.6.1.3 选择器的设计

在双网冗余的核心就是选择器，他的功能如下：

1. 发送数据时，将数据帧复制，在两个网络中同时发送。
2. 接收数据时，如果两个网络都正常工作，接收节点将从两个网络收到两包相同的数据，选择器需要从两个网络中选择一个数据帧，发给节点的应用。选择的机制可以很多，最简单的选择机制是选择最先到达的那个数据帧。如图 3-5 所示，数据帧到达某个 POWERLINK 节点的时序：

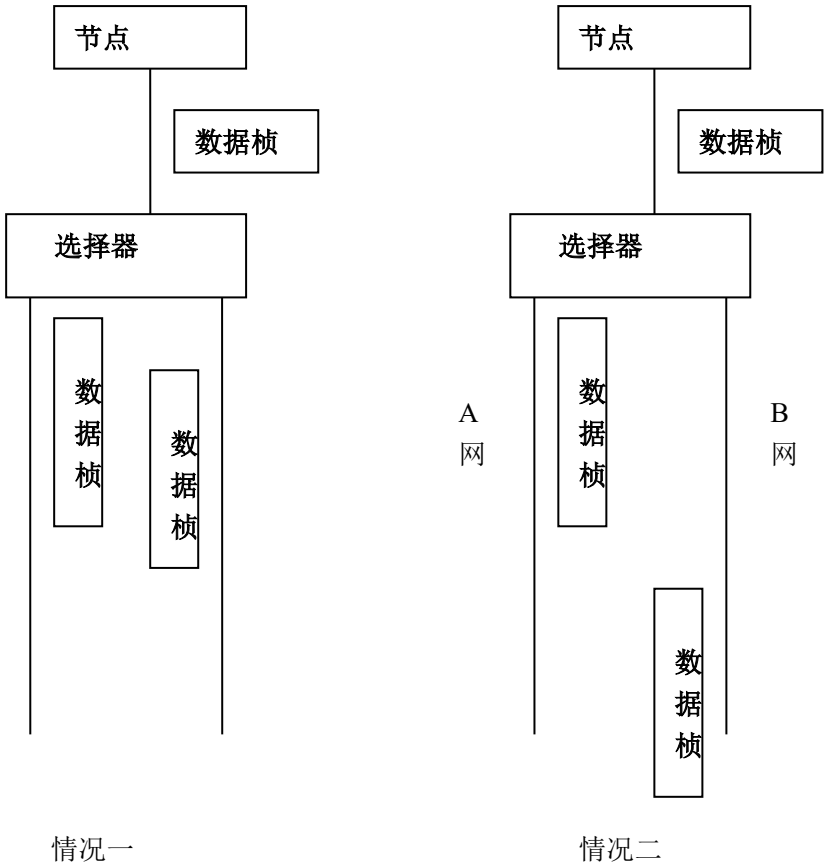

图 3-5 双网中两个相同数据帧的时间差

对于“情况一”，从两个网络上传来的数据帧在时间上交叠在一起，这对于选择器来说，很容易确定这两个数据帧是同样的数据帧，选择最早到来的那个数据帧，丢掉另一个。对于这种网络，要求两个网络对同一个数据帧的延迟时间不能大于一个最小以太网帧传输的延迟（对于 100Mbps 网络来说，这个时间是 5.2 微秒）。如果大于了这个时间，就有可能成为“情况二”。

对于“情况二”，选择器需要首先确定这两帧数据是否为相同的数据帧。因为有可能 A 网过来的数据帧是上一次的老数据，而 B 网过来的数据帧是后一次的新数据，此时 B 网过来数据帧需要传给 POWERLINK 节点。也有可能这两个数据帧是同一数据帧，此时 B 网过来数据帧不需要传给 POWERLINK 节点。对于这种情况如何区分？需要在选择器中缓存先到达的数据帧，将后到达的数据帧和前面缓存的先到达的数据进行比较，如果是相同的，就丢掉后到达的数据帧，否则就需要将后到达的数据帧传给 POWERLINK 节点，同时缓存此帧数据，因为该帧数据为一帧新的数据。

3. 在数据帧中填写线路状态信息。

通过一个选择器（Selector）与两个不同的网络相连。双网冗余支持任意的拓扑结构，树形、星形等。在连接的时候，两个网最好选择同样的 HUB、同样长度的线缆，以保证两个网络的数据包到达某一节点是的时间差不超过 5.2us。

在双网冗余中，每个节点需要一个 Selector，该 Selector 可以集成在节点内部，也可以作为一个单独的设备外接在节点外面。每个节点需要把自己要发送的数据同时发送到两个网络上，这样，接收节点会在两个网络上都能收到该数据包，Selector 的作用就是从这两个数据包中选择一个作为接收的数据,selector 的工作原理如图 3-6 所示。

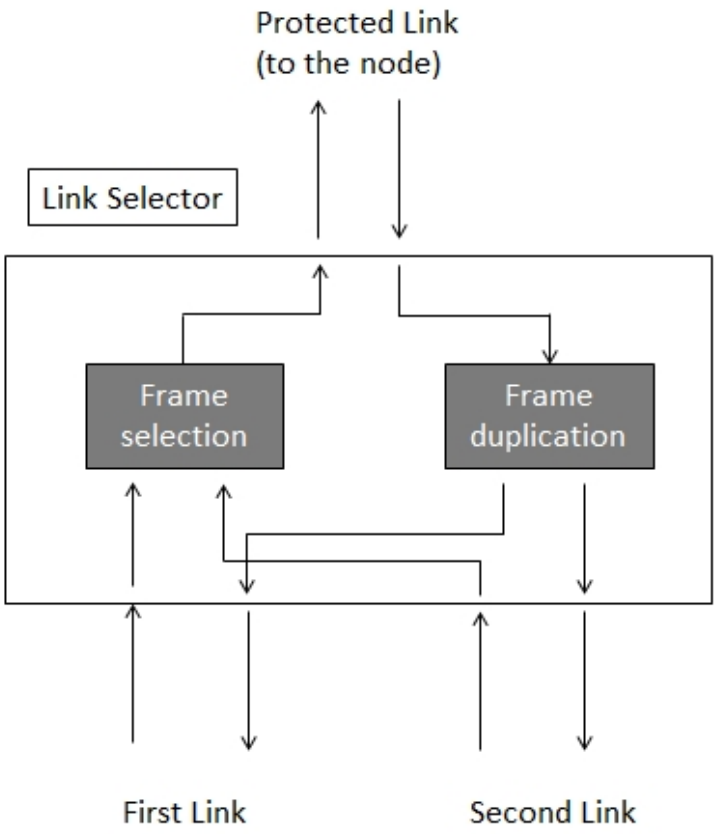

图 3-6 “Link Selector”内部结构

3.6.1.4 双网冗余的 FPGA 解决方案

双网冗余的 FPGA 方案如下：

双网冗余是在单网的 FPGA 方案上，将“openHUB”模块替换为“Link Selector”。使用

FPGA 来实现 POWERLINK 和双网冗余（cable redundancy）的系统架构如图 3-7 所示。

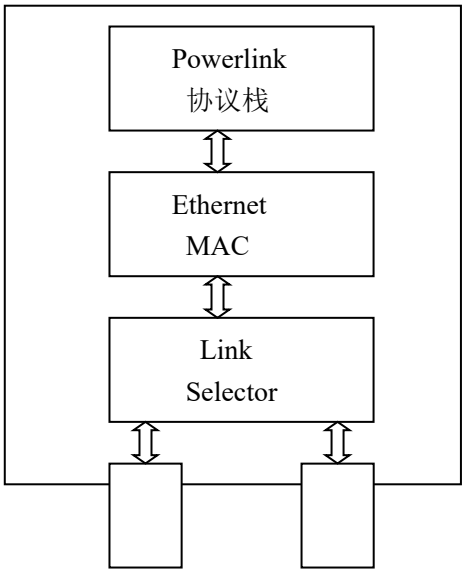

图 3-7 双网冗余的 FPGA 方案

3.6.2 环形冗余

环形冗余是一种常用的冗余，也是一种线路的冗余，当菊花链的拓扑结构的最后一个节点再与主站相连接时，就构成了一个环。当某一根线缆出问题，这个系统依然可以继续工作，但是如果有两根线缆出现问题，就会导致某个或某些节点从网络中分离开。

3.6.2.1 环形冗余的拓扑

非环形冗余的拓扑结构如图 3-8 所示，对于这种拓扑结构，如果某个节点或某段线路出现故障，就会导致部分节点从网络上脱离，例如当 3 号节点出现故障，或者与 3 号节点相连的线缆发生脱落，就导致 4 号和 5 号节点从网络中脱离，而失去连接。

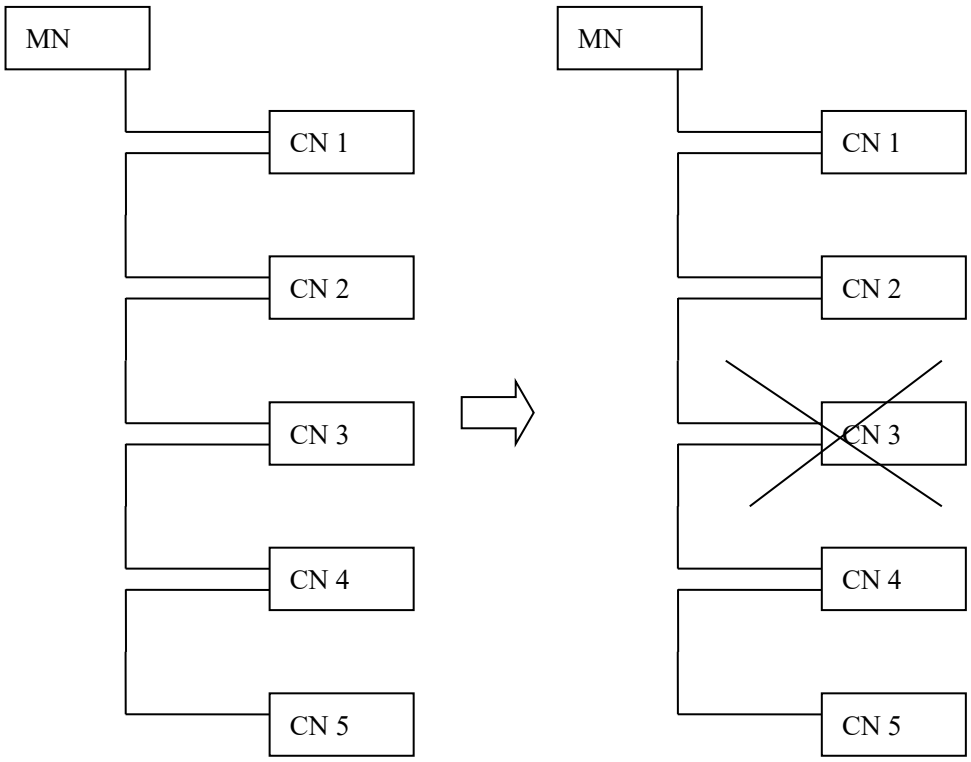

图 3-8 菊花链型的单网拓扑

为此，我们引入了环网拓扑，将最后一个节点和第一个节点用线缆相连，这样整个网络上的节点就构成了一个环，因此称之为环形冗余，如图 3-9 所示。对于这种拓扑，当 3 号节点出现故障，或者和 3 号节点相连的线缆发生脱落，4 号和 5 号节点依然和网络相连。因此环形冗余允许一个节点或者一处网段出现故障。

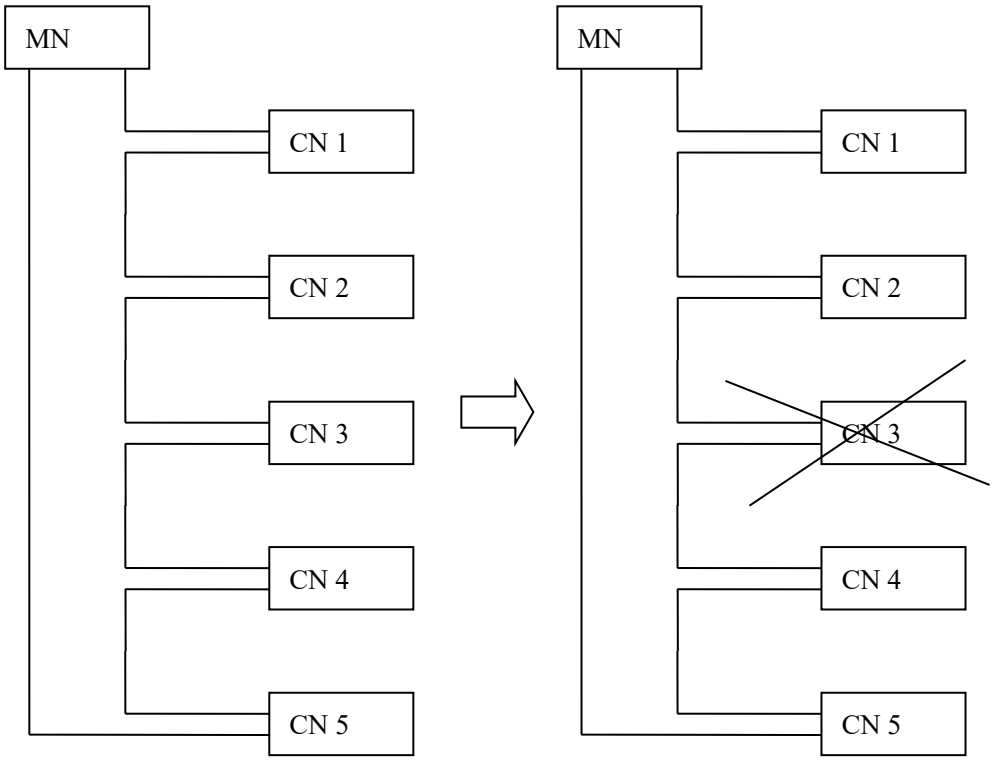

图 3-9 环网拓扑

3.6.2.2 环形冗余的机制

网络闭合时的通信机制：

网络的“环”是闭合的，也就是中间没有断开的点，整个网络形成一个完整的环。

对于环形冗余，有一个节点的模块特殊一些，我们可以称之为“冗余模块”，通常将该模块放置在 POWERLINK 主站节点处，其他节点都是用普通的 HUB。

当主站有数据需要发送时，它从冗余模块的两个网口中选择一个，假定我们选择 B 口，将数据发送出去，如果当前网络的“环”是闭合的，也就是中间没有断开的点。这个数据帧从 B 口发出，经过网络上所有的节点，最后到达冗余模块 A 口。至此，该数据帧已经遍历了网络的所有节点，它的作用已经完成，冗余模块从 A 口接收到该数据帧之后，需要把这个数据帧处理掉，无需再放到网络中传输，否则会形成网络风暴，

在网络上积累的数据帧越来越多，导致系统最终无法运行，如图 3-10 所示。

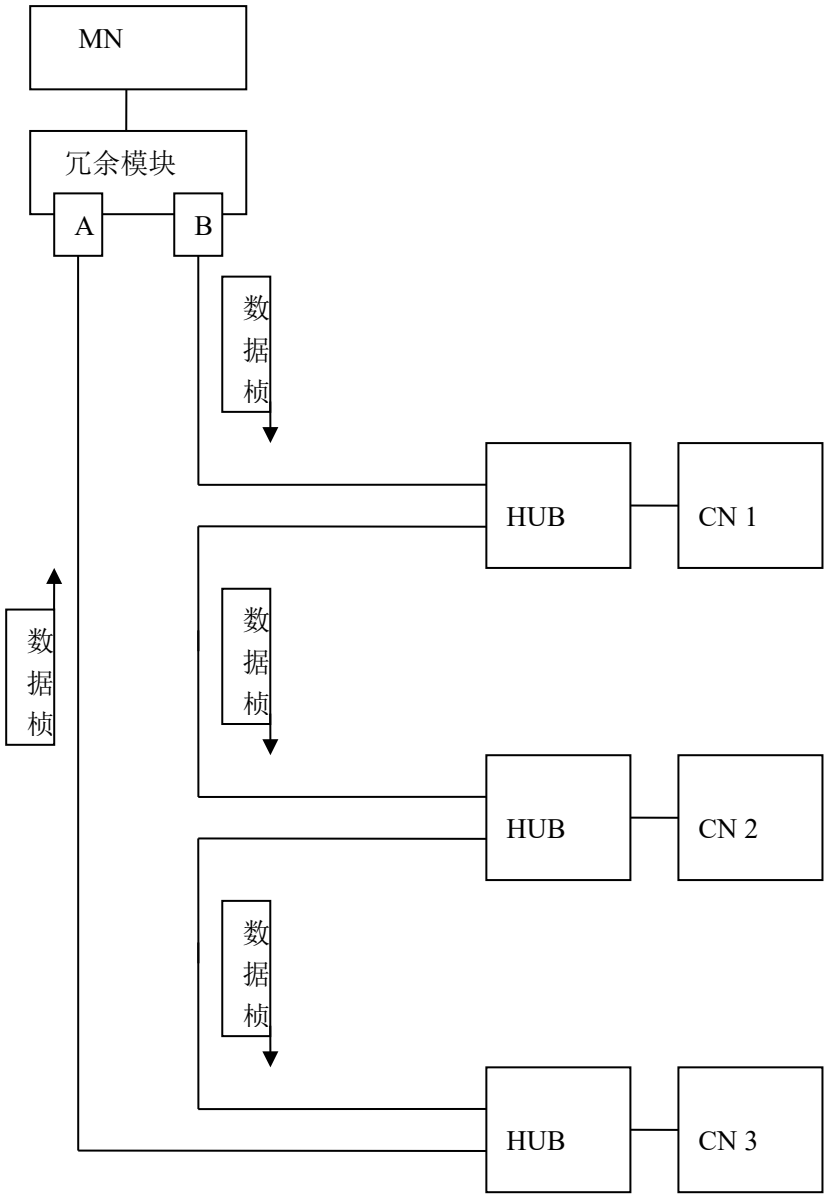

图 3-10 环网冗余主站发送数据

如图 3-11，当某个从站节点发送数据时，例如 2 号从节点，如果当前网络的“环”是闭合的，也就是中间没有断开的点，该节点发送的数据会从 HUB 的两个网口同时发送出去，由于网络没有断点，所以该数据帧在遍历完网络所有节点以后，也会到达冗余模块的 A 口和 B 口，此时它的作用已经完成，冗余模块也需要把这个数据帧处理掉，无需再放到网络中传输。

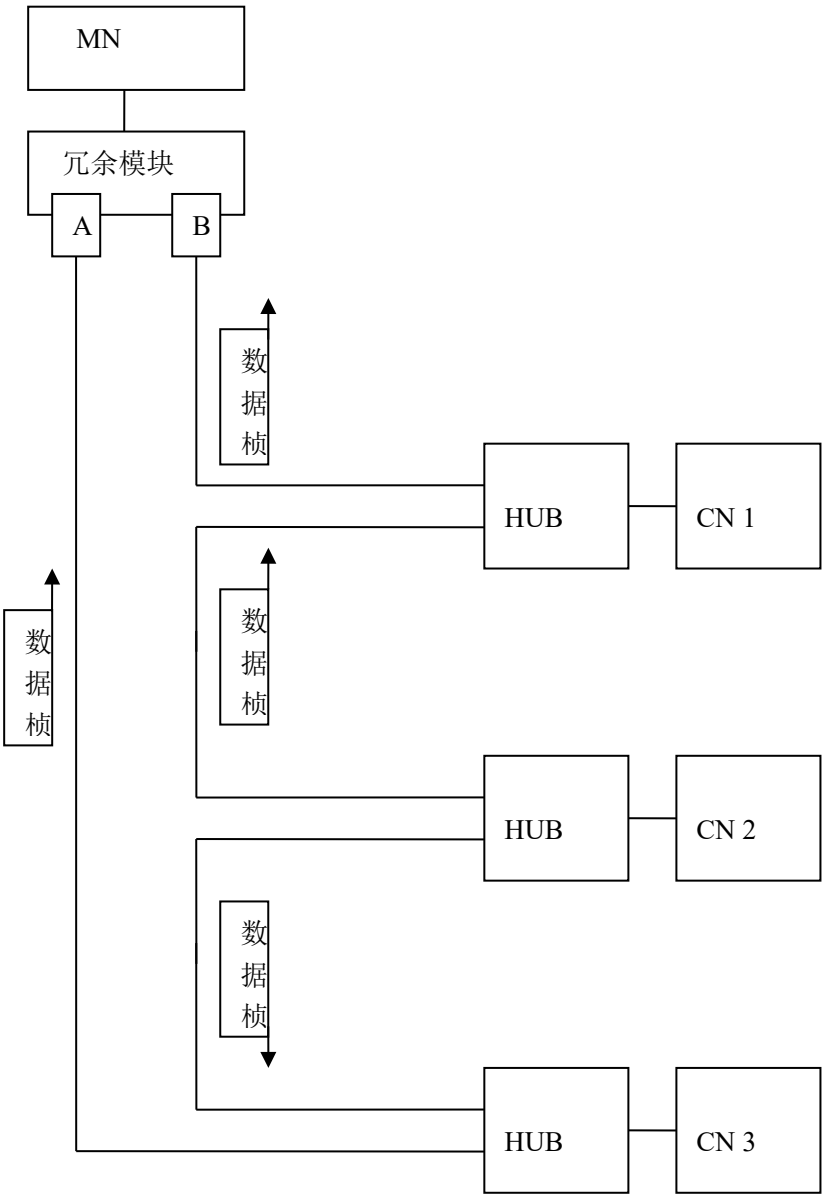

图 3-11 环网冗余从站发送数据

综上，当网络的“环”是闭合的，冗余模块只从一个网口收 / 发数据帧，而另一个网口在收到数据后，将该数据帧吸收掉。

网络开环时的通信机制：

网络开环，也就是网络中有一个断点，使得网络的“环”断开，成为菊花链结构。如下图所示，假如 2 号从节点和 3 号节点之间的网络脱落。 此时冗余模块的作用和 HUB 的功能相同。因为只有这样，才能使网络中的每一个数据帧都遍历整个网络。

因此对于环形冗余，在网络“闭环”时，冗余模块的一个网口用来收 / 发数据，而另一个口用来“吸收”数据；在网络“开环”时，冗余模块就变成了一个 HUB，环网的切换如图 3-12 所示。

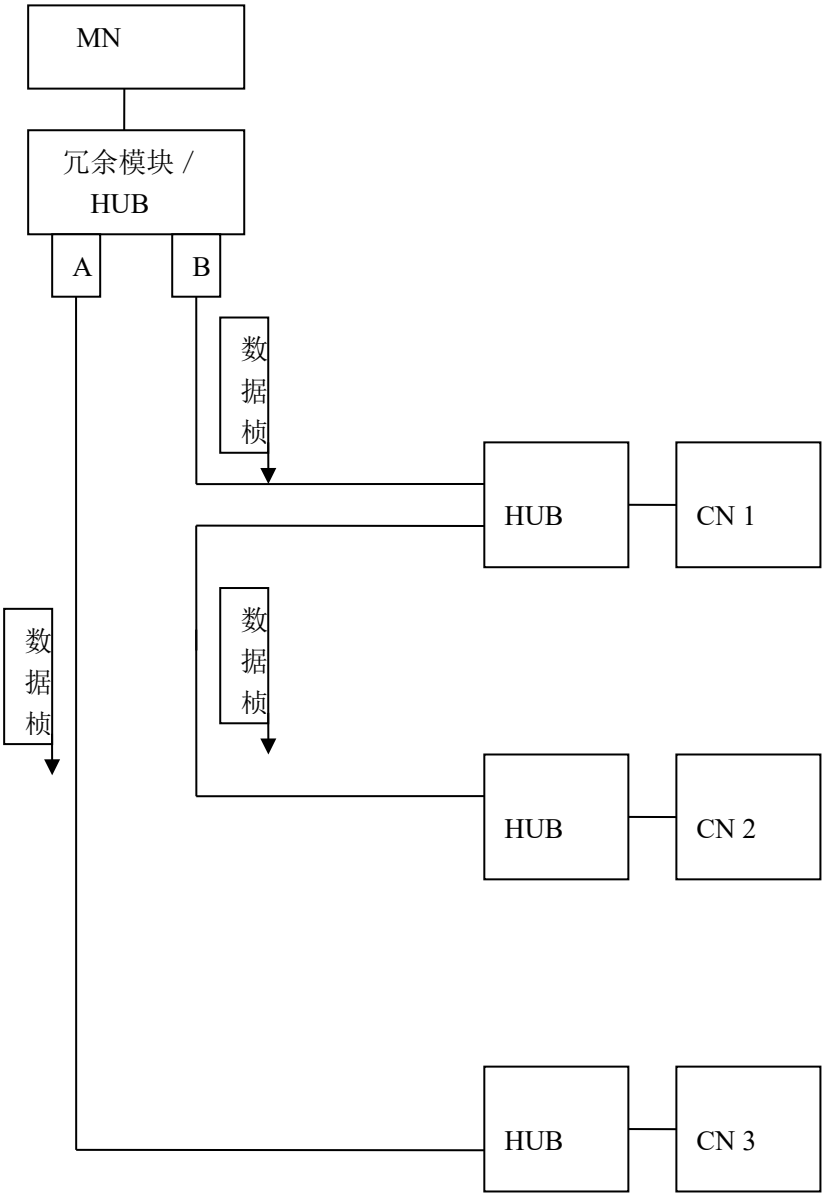

图 3-12 环网冗余网络有断点的处理机制

3.6.2.3 网络状态检测

由于冗余模块的功能在不同的网络状态（开环和闭环）下，功能是不同的，因此冗余模块需要实时监控网络的状态，根据网络的状态来切换自己的功能。

网络闭环状态的检测：

当网络的状态为闭环时，主站从冗余模块网口 B 发出的数据，能达到冗余模块的网口 A，因此检测网络状态是否为闭环最简单的方法就是监控冗余模块的网口 A 是否收到了来之主站的数据帧,即数据帧中的源 node id 的值大于 239。这些数据帧包括：SoA，SoC, PollPreq, PollPresMN, ASND 等，通常采用 SoA 数据帧。

网络开环状态的检测：

当网络的状态为开环时，主站从冗余模块网口 B 发出的数据，不能达到冗余模块的网口A,因此检测网络状态是否为开环最简单的方法就是监控冗余模块的网口A，如果冗余模块的网口 A 在一段时间 T 内没有收到来自主站的数据，说明网络状态为开环。这里最关键是的时间参数 T 的选择，如果 T 选的比较小，就会出现错误的判断，如果 T 选的比较大，就会导致丢失太多的数据帧。时间参数 T 的选取主要取决于网络的传输延迟，即数据帧从冗余模块网口 B 发出，至到达冗余模块网口 A，所经历的时间 T_delay。 当主站从冗余模块网口 B 发出一个数据帧，如果网络是闭合的，那么冗余模块网口 A 应该在时间 T_delay 后收到该数据，如果没有收到，就说明网络是开环的。时间 T_delay 可以通过在冗余模块中实际测量得到。

一种比较简单的算法：冗余模块网口 B 已经连续发送了 2 次的 SoA,但是冗余模块网口 A 还没收到来自主站的数据，这时说明网络状态是开环的。因为冗余模块网口 B 已经连续发送了 2 次 SoA 的时间间隔为一个 POWERLINK 循环周期，数据帧在网络中的传输时间 T_delay 一定小于 POWERLINK 循环周期。否则，意味着主站发送数据至最后一个节点的时间大于一个 POWERLINK 循环周期，这是不可能的。

3.6.2.4 冗余模块状态检测

如前所述，冗余模块的功能和当前的网络状态有关，当网络状态为闭环时，冗余模块的网口 A 需要吸收掉接收到的数据帧，同时不断检测当前的网络状态，当发现网络

状态变为开环，就切换到开环状态；当网络状态为开环时，冗余模块成为一个 HUB，冗余模块的网口 A 就成了 HUB 的一个接口，同时不断检测当前的网络状态，当发现网络状态变为闭环，就切换到闭环状态。图 3-13 为环网冗余状态检测模块的工作状态图：

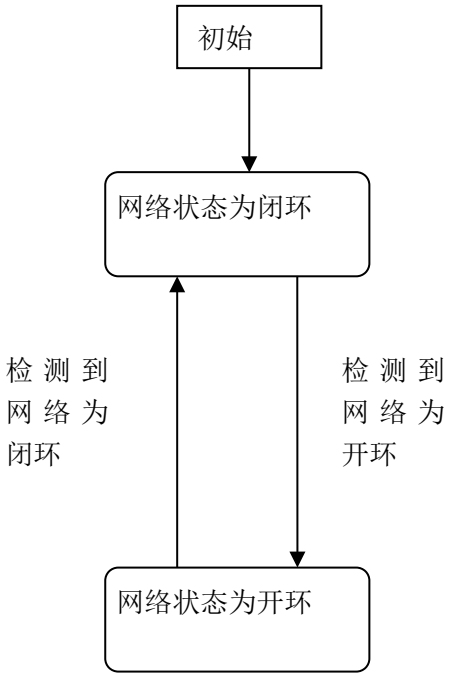

图 3-13 环网冗余状态检测机制

注意：当网络状态从闭环变为开环时，由于检测算法的原因，会导致丢失一个循环周期内的部分数据；当网络状态从开环变为闭环时，由于检测算法的原因，会导致丢失一个循环周期内的部分数据在网络中一直被传递，直到冗余模块的工作状态切换到闭环状态，冗余模块的网口 A 将其吸收为止。

3.6.2.5 链路状态检测

当网络的某个点出现故障时，网络中的节点需要将此信息传递到应用层，方便用户检查并修理故障点。HUB 和冗余模块的每个端口都需要检测对数据帧的接收情况。某个端口如果在一段较长的时间内没有收到数据，说明有可能与该端口连接的网段出现了故障，HUB 或冗余模块需要将该端口的状态信息上报到 POWERLINK 协议栈。

POWERLINK 协议栈中可以定义一个 object 来保存该信息。其他的节点可用通过 PDO 或者 SDO 的方式得到该信息，上报给其他节点的应用程序。

3.6.2.6 环形冗余的无缝切换

此前所讲的环形冗余，网络从闭环状态转变为开环时，会丢失一个循环周期的部分数据; 网络从开环状态转变为闭环时，会导致一个循环周期的部分数据在网络上传输多次，造成网路风暴。也就是说前面的设计方案，在网络状态切换时会造成一个循环周期内的部分数据丢失或多次传输。大部分应用场合，可以接受这样的扰动，而有些应用场合则要求无缝的切换，也就是网络状态切换时，网络通信不受影响。

为了达到无缝切换的效果，我们对 POWERLINK 稍加改动，就可以实现。

环形冗余网络无缝切换的架构如图 3-14 所示：

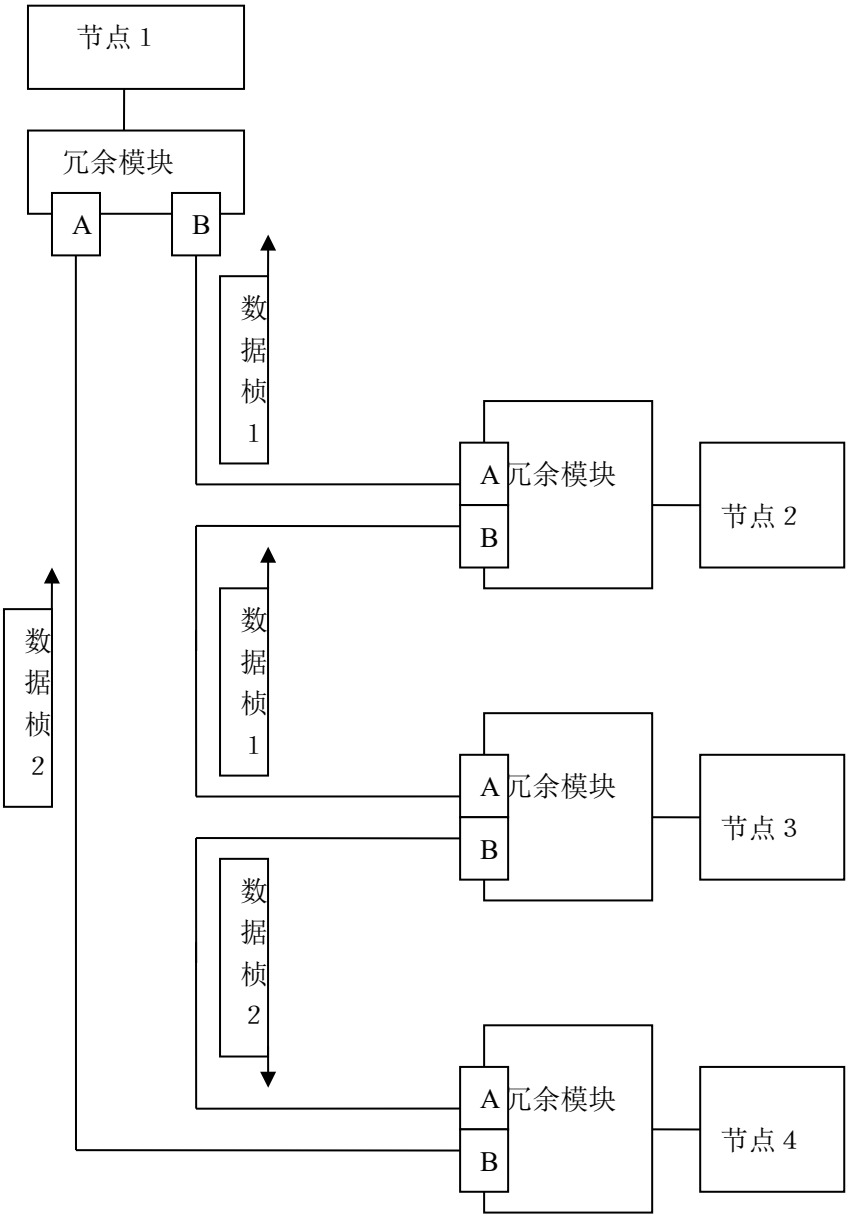

图 3-14 无缝切换的环网机制

图 3-14 描述了节点 3 将要发送的数据帧，从冗余模块的两个端口同时发出，假如这两帧数据同时到达节点 1 的冗余模块，这里约定从端口 A 发出的数据帧为数据帧 1，从端口 B 发出的数据帧为数据帧 2。这两帧数据，就像两列列车，分别沿着顺时针方向和逆时针方向行驶，列车经过的地方，就是数据到达的地方。两列列车，相向而行，必

然会在某一个点相遇，假设数据帧 1 和数据帧 2 在节点 1 处相遇，这时冗余模块从两个数据帧中选择一个上报给与该冗余模块相连的节点，同时数据帧 1 和数据帧 2 中止在网络上传输。由于 POWERLINK 是工作在以太网的半双工模式下，所以一个端口在接收数据的同时，不能发送数据，所以必然会导致数据帧 1 和数据帧 2 在相遇节点处的冲突。

当网络出现某个断点时，例如节点 2 从网络上断开，数据帧 1 和数据帧 2 依然可以遍历网络上所有的节点，只是这两帧数据不会发生碰撞，如图 3-15 所示，网络出现断点时的数据传输路径。

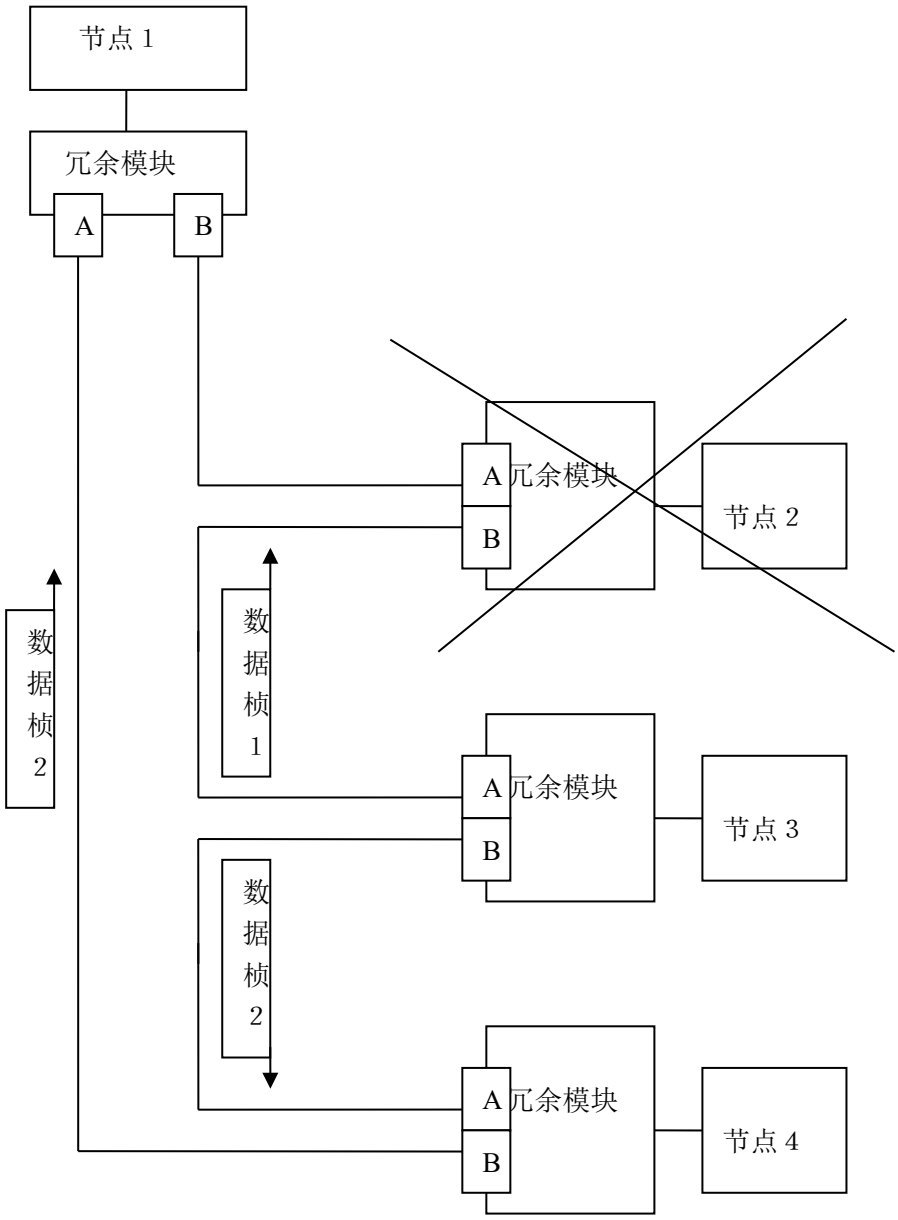

图 3-15 无缝切换的环网中出现断点

对于同时收到的两个相同数据帧， 选择一个上报给与该冗余模块相连的节点，同时中止这两个数据帧在网络上传输。比较简单做法是，当在某个冗余模块中检测到冲突，就选择一个上报给与该冗余模块相连的节点，同时中止这两个数据帧在网络上传输。因为 POWERLINK 的数据帧具有严格的时序，如果不出故障，就不会出现其他情况的冲

突。

3.6.2.7 环网冗余的 FPGA 解决方案

环网冗余是在单网的 FPGA 方案上，将“openHUB”模块替换为“Switch HUB”，如图 3-16 所示。 “Switch HUB”的功能如上所述，根据网络的状态进行切换。

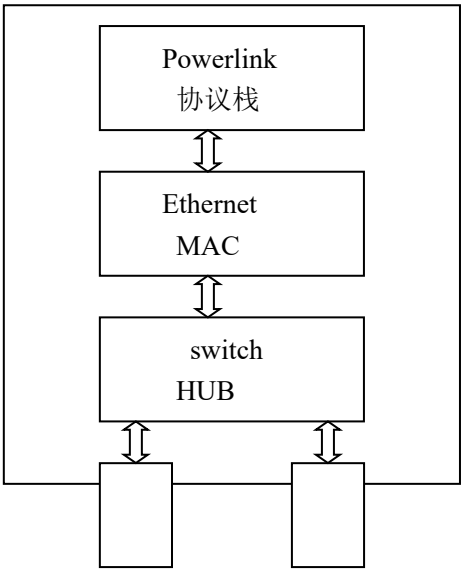

图 3-16 环网冗余的 FPGA 方案

3.6.3 多主冗余

由于一个 POWERLINK 网络有且只有一个 MN，当正在工作的主站出现故障时，网络就会瘫痪，因此对于要求较高的一些场合，需要多主冗余。在一个系统中，存在多个主站，其中一个处于活动状态，其他的主站处于备用状态，当正在工作的主站，出现故障，备用主站接替其工作，继续维持网络的稳定运行如图 3-17 所示。

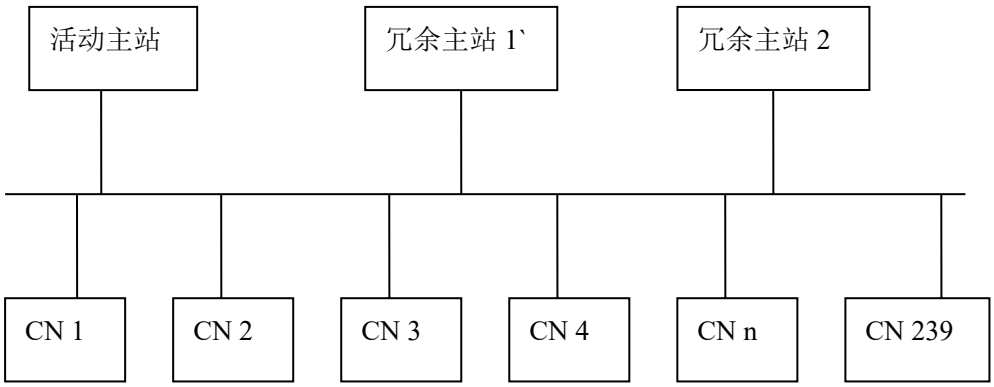

图 3-17 多主冗余的拓扑

3.6.3.1 节点号 NODE ID 的分配

对于 POWERLINK 的从站节点号的范围是从 1 至 239；而对于标准的主站，节点号为 240；对于主站冗余系统，由于有多个主站，这些主站的节点号范围为 241 至 250。

在多主冗余中，无论是活动主站还是备用主站，他们的节点号范围是从 241 至 250。对于活动的主站，在向外发送 SoC, SoA, PollRequest，ASND 数据帧时，将其源 NODE ID 的值设置为 240；在向外发送 PollResponse 数据帧时，数据帧中源 NODE ID 的值设为活动主站自身的 NODE ID。对于备用主站，使用其自身的节点号来收发数据。如下图所示，当节点号为 241 的主站处于活动状态时，他使用 241 和 240 作为自己的节点号，来收发数据，当节点号为 241 的主站出现故障，节点号为 242 的主站接替其工作时，节点号为 242 的主站使用 241 和 240 作为自己的节点号，来收发数据，如图 3-18 所示。

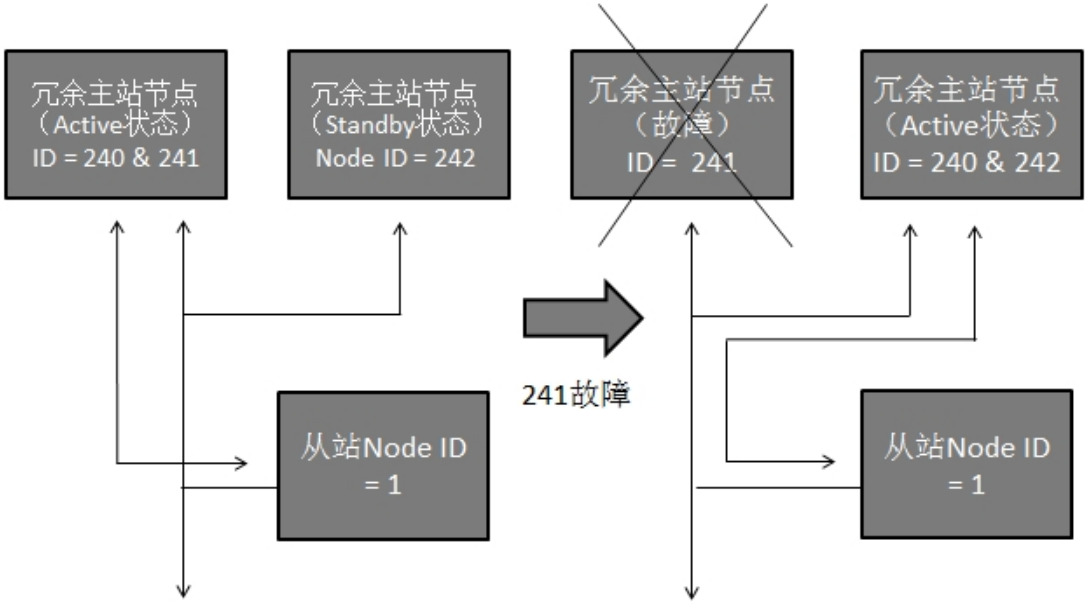

图 3-18 多主冗余的主站切换示意图

当活动主站从 MN1 切换到 MN2 时，MN1 和 MN2 发送的数据帧的目标 MAC 地址和 POWERLINK 源地址，目标地址值的变化，如图 3-19 所示，描述了冗余的活动主站（MN1）和冗余的备用主站(MN2),以及从站(CN1)在通信过程中的“源 MAC”地址和“目标 MAC”地址分配。

“Message Type”：数据帧的类型

“MAC Source”：数据帧的源 MAC 地址

“MAC Destination”： 数据帧的目的 MAC 地址

“POWERLINK src”：数据帧的源 Node ID

“POWERLINK dest”：数据帧的目标 Node ID

MAC Source	MAC Destination	Message Type	POWERLINK src	POWERLINK dest
MAC-MN1	01:11:1E:00:00:01	SoC	240	255
MAC-MN1	MAC-CN1	PollRequest	240	1
MAC-CN1	01:11:1E:00:00:02	PollResponse	1	255
MAC-MN1	MAC-MN2	PollRequest	240	242
MAC-MN2	01:11:1E:00:00:02	PollResponse	242	255
MAC-MN1	01:11:1E:00:00:02	PollResponse	241	255

MAC-MN1	01:11:1E:00:00:03	SoA	240	255
Switch-over, MN2 becomes active				
MAC-MN2	01:11:1E:00:00:01	SoC	240	255
MAC-MN2	MAC-CN1	PollRequest	240	1
MAC-CN1	01:11:1E:00:00:02	PollResponse	1	255
MAC-MN2	MAC-MN1	PollRequest	240	241
MAC-MN1	01:11:1E:00:00:02	PollResponse	241	255
MAC-MN2	01:11:1E:00:00:02	PollResponse	242	255
MAC-MN2	01:11:1E:00:00:03	SoA	240	255

图 3-19 多主冗余主站发送数据帧的 MAC 地址分配

3.6.3.2 配置管理

主站的对象字典中保存了对网络上所有从节点和冗余主站的配置信息。当网络上电以后，主站首先检查是否需要配置网络上的其他节点，如果需要，就根据保存在主站内的配置信息通过 SDO 的方式发送给相应的节点。当某个节点重新回到网络中时，主站也会去检查是否需要重新配置该节点。因此活动主站从 MN1 切换到 MN2 时，MN2 的对象字典里也需要保存有与 MN1 相同的对网络上节点的配置信息，配置示意图如图 3-20 所示。

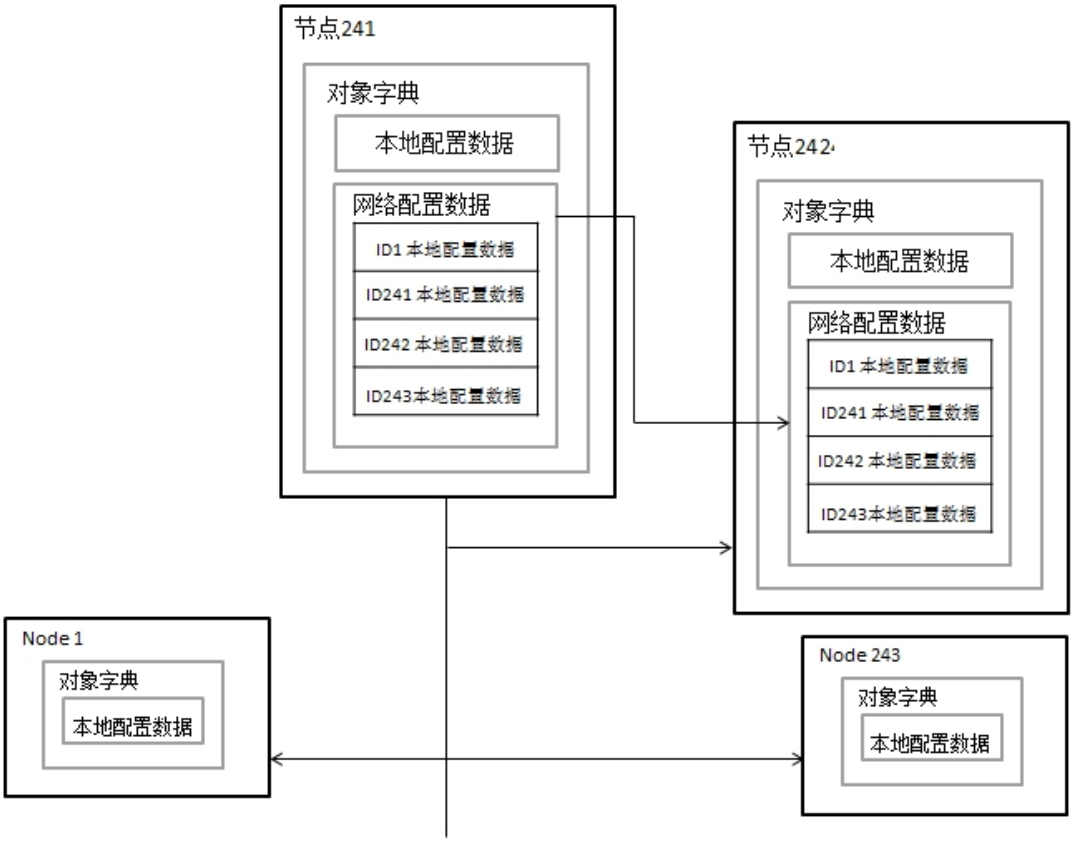

图 3-20 多主冗余网络配置信息

3.6.3.3 接管仲裁

由于在一个系统中有多个备用主站，当活动主站出现故障时，需要有一种机制，从多个备用主站中选择一个接替活动主站的工作。这里采用竞争机制，每个备用主站有唯一的优先级，这个优先级有两种方式确定：

1．在备用主站中定一个 object，用来保存优先级参数，这个 object 的索引为 0x1f89,子索引为 0x0a。在组建 POWERLINK 网络时，事先配置好每个备用主站的优先级。优先级是一个数值，取值范围为 1，2……等自然数。数值越小，优先级越高。

2．由节点号来确定优先级。由于每个备用节点有唯一的节点号，可以将节点号的数值看作是优先级的值。

系统上电时，多个冗余主站同时启动，此时哪个冗余主站应该率先接管网络，成为活动主站？这由前面所说的优先级决定。所有冗余主站根据优先级的不同，分别等待不同的时间。如果在等待的时间内收到了 SOA 数据帧，说明已经有其他的主站开始工作，

该冗余主站进入 standby 状态；如果在等待的时间内没有收到 SOA 数据帧，该冗余主站进入活动主站状态，进入 Reduced Cycle。由于 POWERLINK 主站在启动的时候，首先进入到 Reduced Cycle, 在这个状态下，主站只是产生 SOA 和 ASND 来配置网络。如果活动主站在这个正在工作在该状态下，由于某种故障停机，备用主站需要有能力检测，并根据优先级的机制选出一个备用主站，接替活动主站的工作。因此当活动主站工作在 Reduced Cycle 状态时，备用主站需要周期性检测 SOA，如果很长时间没有收到 SOA，就认为活动主站出现故障。具体的方法是在备用主站中实现一个定时器。定时器的定时时间为 T_reduced_switch_over_MN 是指如果在该时间间隔内没有收到 SOA，就认为网络中没有活动的主站来产生 SOA。备用主站每次收到 SOA 数据帧，就重新设置自己的定时器；如果定时器的定时时间到，但是还没收到 SOA 数据帧，就启动接管程序。启动接管程序时，首先发送一个广播消息 ActiveManagingNodeIndication (AMNI)，来通知网络上其他的备用主站，本主站将要成为活动主站。其它的备用主站，在收到该消息时，需要重新设置自己的定时器，启动过程如图 3-21 所示。

优先级高的备用主站，T_reduced_switch_over_MN 的时间小，这样的备用主站等待时间短，优先级低的备用主站，T_reduced_switch_over_MN 的时间大，定时器等待的时间长。

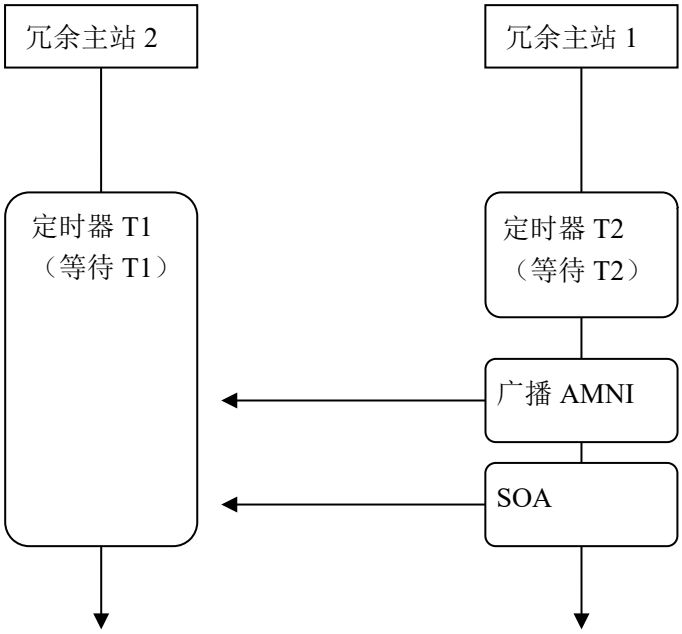

图 3-21 多主冗余的启动过程

冗余主站 1 的优先级高，等待的时间短，当定时结束后，还没有收到 SOA/SOC 数据帧，会发送广播 AMNI 数据帧，通知其他冗余主站，将由本站做为活动主站。冗余主站 2 的优先级高，等待的时间短，当定时结束后，冗余主站 2 收到了 AMNI 数据帧或者 SOA 数据帧,这时冗余主站 2 将进入到" standby"状态，备用主站接管网络管理权的过程如图 3-22 所示。

注意在启动时，这里的 T1，T2 要设置的足够长，以便有明显的优先级，如果|T1-T2|的值太小（例如几个微秒），由于冗余主站 1 和冗余主站 2 在上电顺序，初始化的速度等差异，导致两个设备不能同时启动定时器，从而使优先级失效，因此最好把这两个参数设置的大一些，而且之间的差值也足够大。

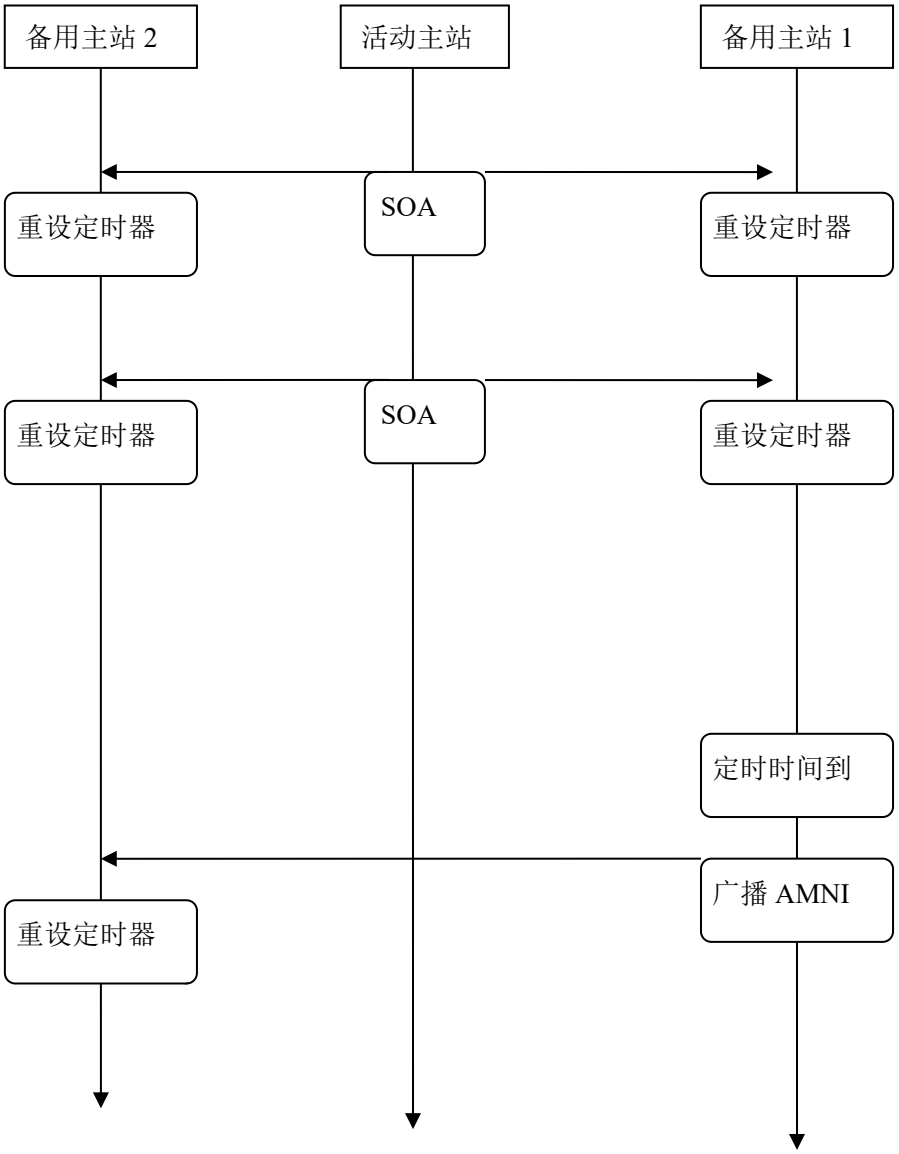

图 3-22 多主冗余的监控机制

当活动主站进入到 POWERLINK 正常的循环周期，会周期性产生 SOC 数据帧。在该状态下，备用主站需要检测 SOC 数据帧，如果很长时间没有收到 SOC 数据帧，就说明当前的活动主站出现故障，优先级最高的备用主站将接替活动主站的工作。备用主站检测 SOC 数据帧的方法依然是通过设置定时器。定时器的值如下:

$$T_{switch_over_MN} = T_{cycle_MN} + \frac{T_{cycle_MN} * (MNSwitchOverPriority_U32 + MNSwitchOverDelay_U32)}{MNSwitchOverCycleDivider_U32}$$

Tcycle_MN 是 POWERLINK 循环周期长度

MNSwitchOverPriority_U32 是节点的优先级，优先级越高，该数值越小。

MNSwitchOverDelay_U32 是一个可选的延时参数，该参数不是必须的。

MNSwitchOverCycleDivider_U32 是一个除数因子，他将循环周期等分，得到较小的时间片。

在主站进入到 operational 工作模式时，之所以采用监控 SOC 数据帧而不是 SOA 数据帧，原因是 SOC 数据帧的抖动更小，更准确。

对于备用主站，每次收到 SOC 数据帧时，定时器清零重新启动。当某个备用主站的定时器定时时间到，说明该备用主站超过一个循环周期没有收到 SOC 数据帧，意味着活动主站可能已经出现故障（但是也不排除如下两种可能：SOC 抖动过大和 SOC 数据帧丢失）。每个备用主站，由于优先级不同，所以每个备有主站的定时器设置的时间不同。当某个备用主站的定时时间到，它就发送一个 AMNI 消息来通知网络上的其他备用主站，本备用主站将要接替活动主站的工作，其他备用主站收到 AMNI 消息，需要将自身的定时器清零重新设置。下面举例说明：

假设在我们的系统里有 3 个冗余主站 RMN (POWERLINK node-ID 241, 242, 243) ，241 是活动主站，假设他现在出现了故障，仲裁机制启动：

RMN241

MNSwitchOverPriority_U32 = 1

MNSwitchOverCycleDivider _U32 = 3

RMN242

MNSwitchOverPriority_U32 = 2

MNSwitchOverCycleDivider _U32 = 3

RMN243

MNSwitchOverPriority_U32 = 3

MNSwitchOverCycleDivider _U32 = 3

下面是各个备用主站的定时器定时时间：

$$T_{switch_over_MN241} = T_{cycle_MN} + \frac{T_{cycle_MN} * (1+0)}{3} = T_{cycle_MN} + \frac{T_{cycle_MN} * 1}{3}$$

$$T_{switch_over_MN242} = T_{cycle_MN} + \frac{T_{cycle_MN} * (2+0)}{3} = T_{cycle_MN} + \frac{T_{cycle_MN} * 2}{3}$$

$$T_{switch_over_MN2431} = T_{cycle_MN} + \frac{T_{cycle_MN} * (3+0)}{3} = T_{cycle_MN} + \frac{T_{cycle_MN} * 3}{3}$$

图 3-23 为接管的时序图。当 242 号备用主站在规定的时间内没有收到 SOC 数据帧，就发送一个 AMNI 消息，然后接管活动主站的工作。243 号备用主站收到 AMNI 消息后，将定时器清零重新设置。

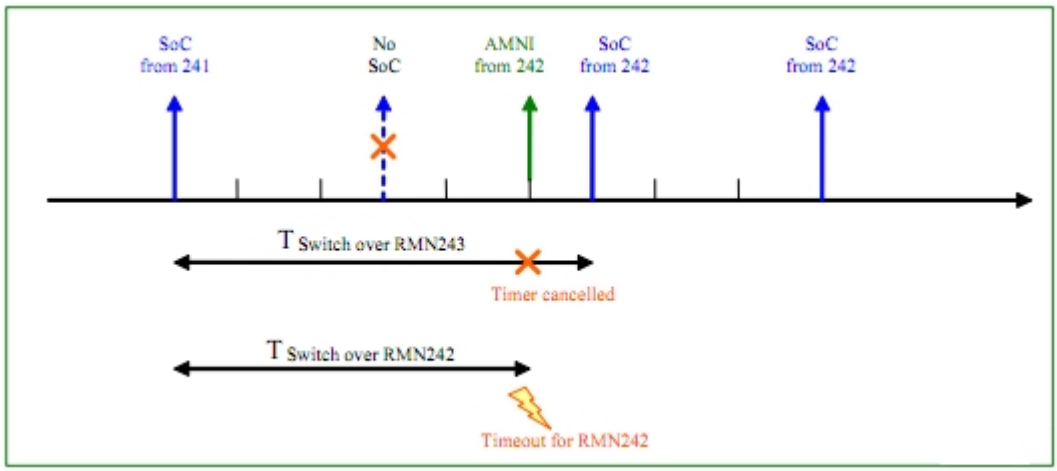

图 3-23 多主冗余备用主站接管时序图

除此之外，应用程序可以通过发送命令让本地或者远程的活动主站进入到 standby 状态。

3.6.3.4 状态切换

1. 启动：POWERLINK 设备在启动时，根据节点号和 NMT_StartUp_U32 object (index 1F80h)的设置来决定该节点接下来的行为。如果该节点的节点号为 1 至 239，那说明该节点是从站，接下来应该进入到从站的状态机。如果节点号是 240 且 NMT_StartUp_U32 object (index 1F80h)的第 14 bit 为 0，则说明该节点是标准的主站。如果NMT_StartUp_U32 object (index 1F80h)的第 14 bit 为 1，则说明该节点是冗余主站，进入到冗余主站的状态机，支持冗余功能的主站的 NMT 状态机如图 3-24 所示。

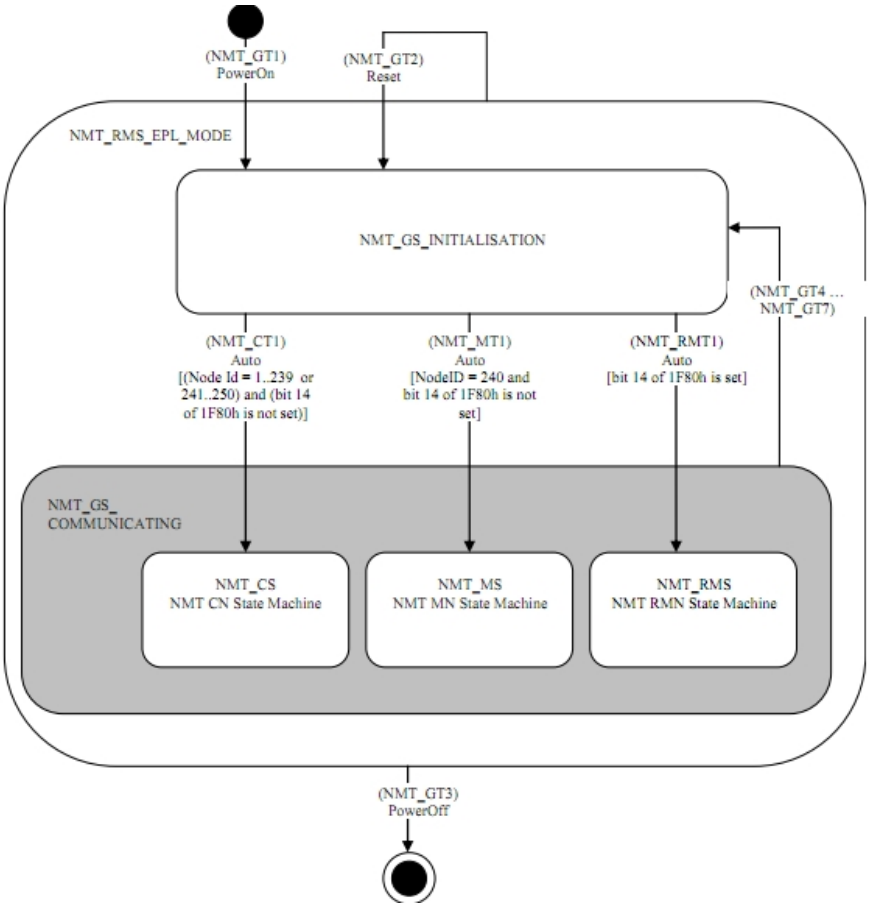

图 3-24 冗余主站的 NMT 状态机

2. 冗余主站的状态机

冗余主站的状态机主要有两个大的状态，一个是 active 状态，一个是 standby 状态。当处于活动状态时，该节点作为活动的主站在工作。当处于 standby 状态时，该节点处于备用主站。当节点启动完成，进入到冗余主站的状态机时，首先检测是否能在规定的时间内受到 SOC 和 SOA 数据帧，如果能收到，说明在网络上有其他的活动主站，该节点应该进入到 standby 状态；否则进入到 active 状态。在 COMMUNICATING 状态下的冗余主站的 NMT 状态机如图 3-25。

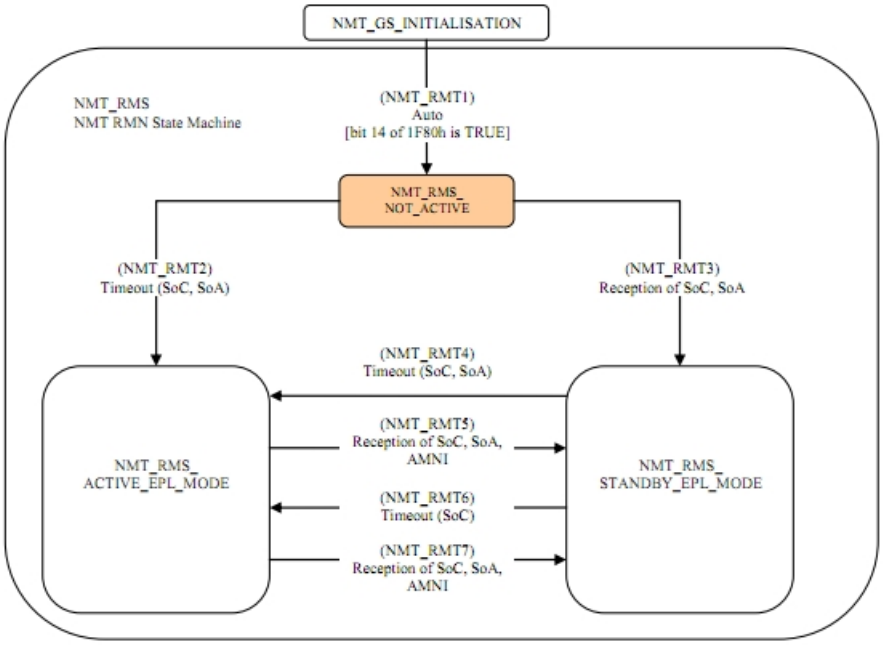

图 3-25 COMMUNICATING 状态下的冗余主站 NMT 状态机

Active 状态：

当节点工作在冗余主站的 Active 状态时，他的作用和标准的主站一样。此外增加了切换到 standby 状态的功能。当该节点收到了 SOC,SOA,AMNI 等消息时，就从 Active 状态切换到 standby 状态。

standby 状态：

当节点工作在冗余主站的 standby 状态时，从活动主站的角度看，备用主站的就像标准的从站那样工作，从活动主站接收 PollReq 数据帧，回复 PollRes 数据帧。此外他还具有如下功能：

定时检测 SOA 和 SOC 数据帧。如果在规定的时间内没有收到 SOA 和 SOC，需要切换状态，接管活动主站的工作。冗余主站切换时的状态机描述如图 3-26 所示。

监控网络上其他节点的状态，备用主站通过监听节点的 PollResponse，StatusResponse，IdentResponse 这些数据帧的信息来得知其状态信息，并将这些信息更新到自己的列表中。在接管活动主站的工作时，需要这些信息，来达到无缝切换。

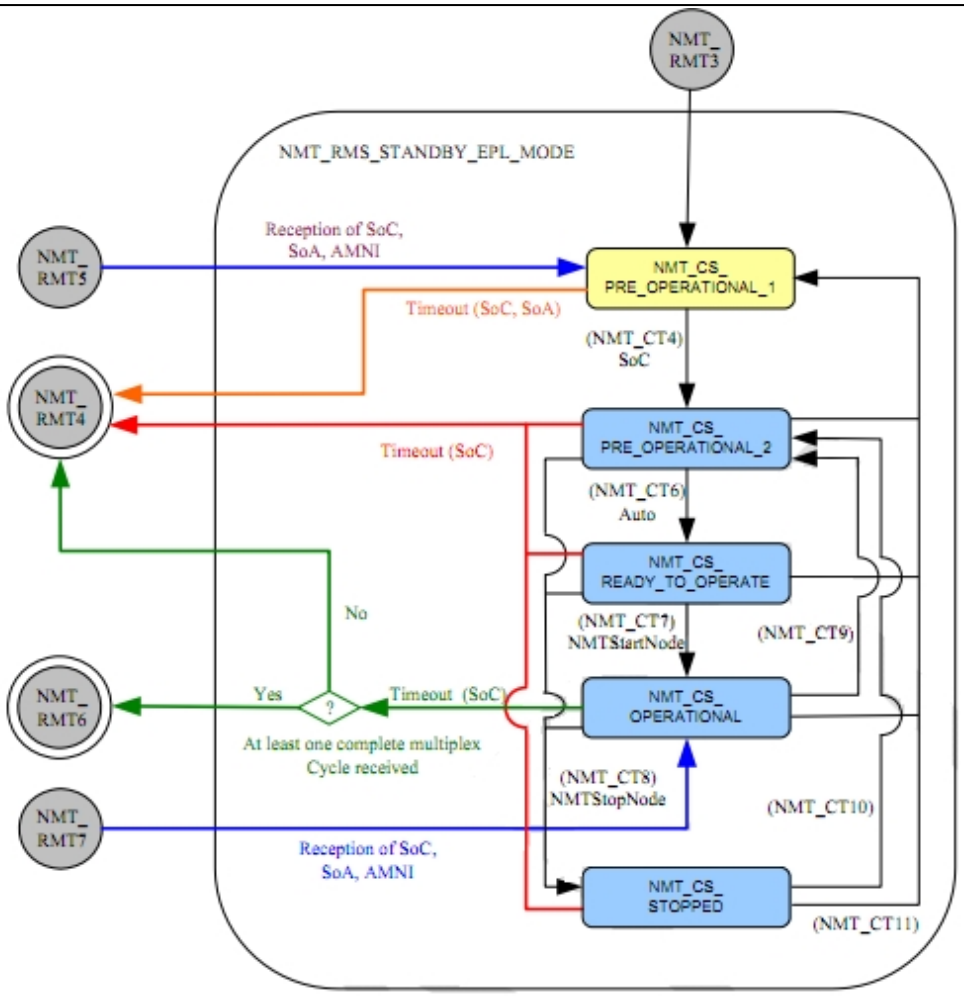

图 3-26 多主冗余状态切换

3.状态切换

表 3-1 所示为状态切换的条件和事件：

NMT_RMT1	Auto ： 自动跳转
	无需任何条件
NMT_RMT2	Timeout SoC, SoA：SoC 或 SoA 超时
	在规定的时间内没有收到 SoC 或 SoA
NMT_RMT3	Reception of SoC, SoA：收到了 SoC 或 SoA
	在规定的时间内收到 SoC 或 SoA
NMT_RMT4	Timeout(SoC,SoA)：SoC 或 SoA 超时

	在“规定的时间”内没收到 SoC 或 SoA ，所谓的“规定的时间”为 Treduced_switch_over_MN resp. Tswitch_over_MN.
NMT_RMT5	Reception of SoC, SoA or AMNI.：接收到 SoC 或 SoA 或 AMNI
	在“规定的时间”内收到 SoC 或 SoA ，所谓的“规定的时间”为 Treduced_switch_over_MN resp. Tswitch_over_MN.
NMT_RMT6	Timeout(SoC)：SoC 超时
	在“规定的时间”内没收到 SoC ，所谓的“规定的时间” Tswitch_over_MN
NMT_RMT7	Reception of SoC, SoA or AMNI：接收到 SoC 或 SoA 或 AMNI
	在“规定的时间”内收到 SoC 或 SoA ，所谓的“规定的时间”为 Tswitch_over_MN

表 3-1 切换条件和事件说明

3.6.4 冗余系统的典型拓扑结构

3.6.4.1 多主环网

多主环网，即在一个环形网络中，存在多个主站，拓扑如图（3-27）：

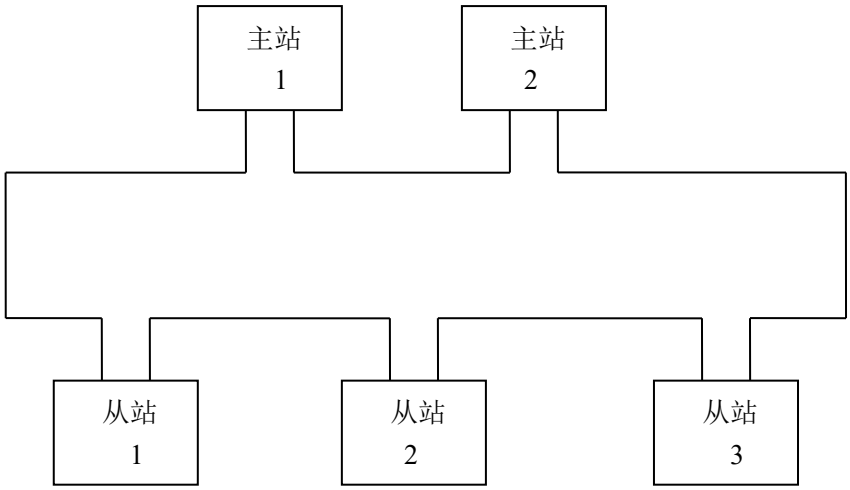

图 3-27 多主环网拓扑图

3.6.4.2 多主双网

多主双网，即在双网的架构中，存在两个或者多个冗余主站，拓扑如图（3-28）：

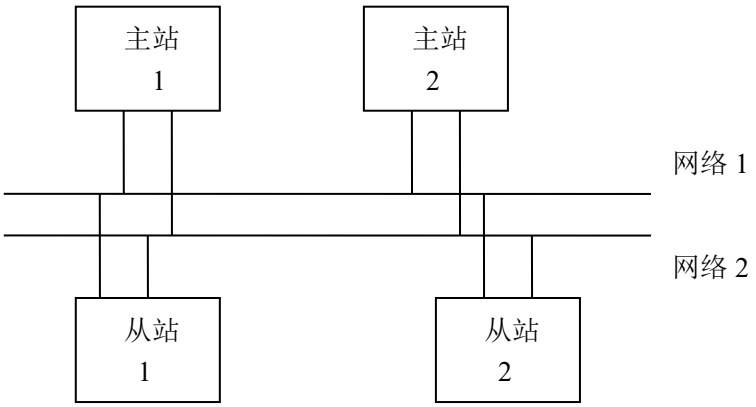

图 3-28 多主双网拓扑图

3.6.4.3 多主双环网

多主双环网即将以上多主，环网，双网相结合，拓扑如图（3-29）：

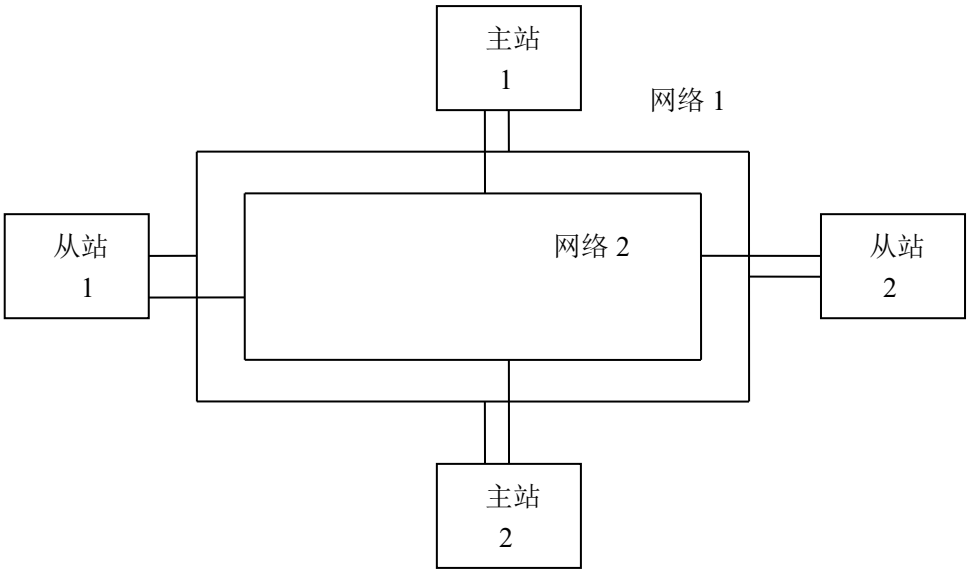

图 3-29 多主双环网拓扑图

3.7 交叉通信

交叉通信是指从站间具有无需通过主站而交换数据的能力。

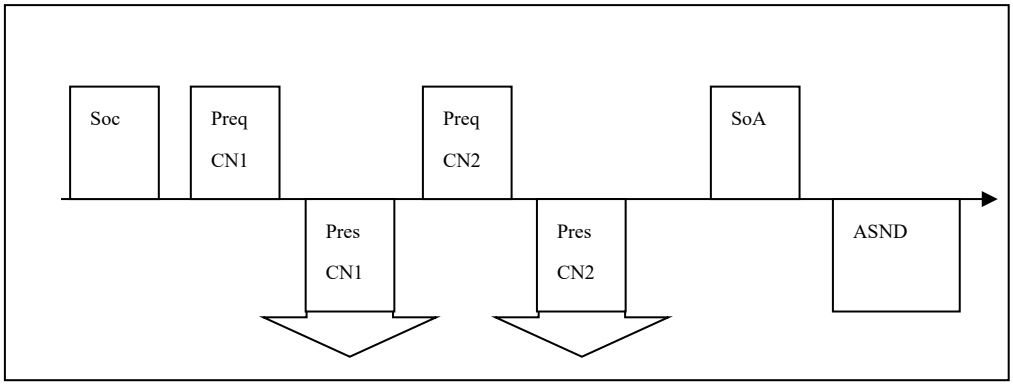

图 3-30 交叉通信的原理

如图 3-31，由于每个从节点在向外发送数据时，都是以广播的形式发送出去，因此网络上的所有节点都可以在本周期内收到，如果其中某个节点需要该数据，那么就可以直接收取。例如 CN1 将自己的数据放在 PresCN1 中，以广播的方式发送出去，主站和其他所有的从站都可以收到该数据包，如果 CN2 需要接收 CN1 的信息，就可以直接收取该数据包的某一段或者某几段数据，而无需经过主站。

交叉通信的好处：

- 集中或分布式控制设计
- 控制器－控制器通信
- 主轴直接给从轴设定值
- 编码器值的直接传递
- 直接事件传播
- 减少主站负载或者应用负载
- 多种模式，最小的数据负载
- 具有分散式安全设计

其他系统不能给用户这些优点，因为它们不支持直接交叉通信，即使这本来就是标准以太网基本属性。

3.8 实时域与非实时域

POWERLINK 网络是一个实时网络，POWERLINK 网络中各个节点的通信，有着严格的时序性。各个节点在哪个时间段得到总线的使用权，是由主站统一分配的。

经常会有人问，我们现在有一个局域网，在这个网络中，有一些非 POWERLINK 的设备，我想让 POWERLINK 的网络共用我的这个局域网，是否可以？

答案是：可以，也不可以。

可以，是因为 POWERLINK 网络，就是基于标准以太网的，因此 POWERLINK 的设备可以与其他以太网设备共存，而且可以相互通信。

不可以，是因为 POWERLINK 网络中，每个站什么时候收发数据，是由 POWERLINK 主站管理的，现在接入了一些非 POWERLINK 的设备，这些设备收发数据，不受 POWERLINK 主站管理。这就会造成冲突，即 POWERLINK 的设备想要发送数据，却发现当前总线被非 POWERLINK 的设备使用。从而造成 POWERLINK 设备通信超时或者数据丢失，产生一些通信报警和错误。

因此正确的做法是实时控制网络与非实时控制网络分开，可以通过网关隔开，或者使用两个不同的网络。

3.9 基于 POWERLINK 的功能安全

openSAFETY 是基于 POWERLEINK 的安全协议，它是一个技术开放，源代码开源

的安全协议。它不单可应用于 POWERLINK，而且可以应用于其它各种实时以太网之上，如 Profinet，Modbus，EthernetIP，以及普通的以太网。

3.9.1 适用于所有现场总线

由 ESPG 引入的 openSAFETY，是世界上第一个 100%开源的安全协议。它不仅在法律层面上是开放的，在技术层面上也是开放的。由于该协议独立于总线，openSAFETY 可以应用于任何现场总线和工业以太网的方案中，甚至用于特殊定制的协议方案中，如图 3-31 所示的 openSAFETY 的网络结构， 在一个 openSAFETY 域里，可以支持各种总线协议。

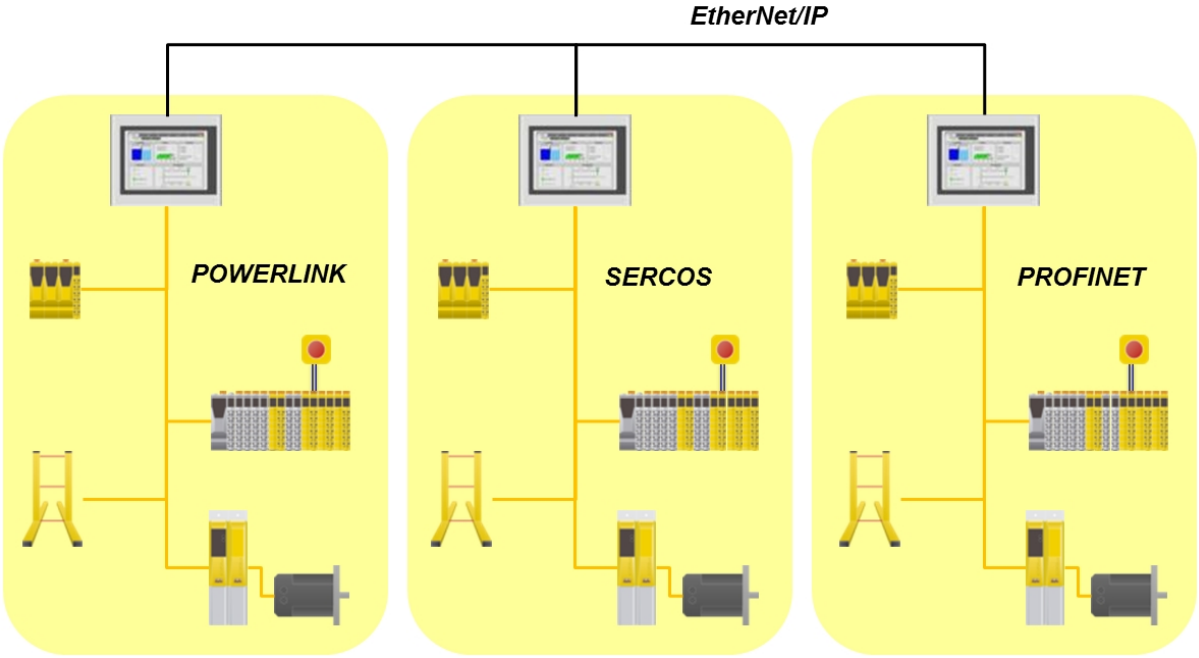

图 3-31 openSAFETY 的网络拓扑

openSAFETY 是第一个开源、独立于总线的安全标准，适用于所有工业以太网方案。

对于在任何数据传输协议上 openSAFETY 的实施，**EPSG 都将提供积极支持，同时也提供认证和一致性测试。经过 TÜV 认证的协议栈确保了对该技术的投资是绝对安全的。**

- 一个统一标准，适用于所有现场总线
- 从站间直通信（**cross communication**）使生产力最大化
- 研发、维护时间进一步减少
- 自动的安全参数化
- 完全符合机器的安全模块化思想
- 完整的开源解决方案
- 最稳健的 **IEC 61508 SIL3** 通信方案
- 无风险，**TÜV** 认证的一致性测验
- 完全适用背板总线

3.9.2openSAFETY 原理

OpenSAFETY 值得人们注意的是数据传输定义以及它提供的高层配置服务、尤其是对安全相关数据的封装，使之成为灵活的报文格式。实际上，在所有应用中，openSAFETY 都使用统一格式的帧，无论是用于负载数据的传输，还是用于配置或时间同步信息。帧长度可变且经济，主要还是取决于要传输的数据量。网络上的安全节点自动识别其内容，即不必配置帧类型和帧长度。

自动的安全参数分配

openSAFETY 的亮点之一就是自动的安全参数分配：该协议可以进行安全应用的详细配置信息的存储，例如安全控制器中的光幕。如果一个设备要换下，安全控制器会自动并准确无误地将存储的配置信息下载到换上的应用中。即，当用户换掉下一个安全设备后，用户无需手动配置新节点。

故障可靠检测

openSAFETY 通过校验和来检查是否存在不完整的数据传输，以及对于数据传输率的常监视。因为循环时间是非常短的，错误几乎没有任何延迟便可检测到。由于所有数据通信的一场都能被识别，甚至非安全网络无法兼容安全向功能。
下图指出可能会发生哪些错误，并解释 openSAFETY 使用的用以便是和防止故障的机制。

故障原因

数据传输错误中的很大比例是网关转发时出的错。假若两个网络之间有两个网关，传输了相同的数据，那么数据重复便可能发生。另一方面，如果网关没有转发数据，或者转发到其他网络上，那么数据包就丢失了。如果数据包可以根据长度需要，以一个部分包序列传输，那么因路径不同、网关各式各样，造成数据包的一些段的顺序错误和混淆。网关的数据转发也会因其负载过高而延迟。
另一个数据出错源头是电磁干扰。它可能导致数据位翻转，甚至破坏真个信息段。再者，在传输标准数据和安全数据的网络上，还会出现“数据伪装”（masquerades），即因错序和混淆导致标准信息被错当成安全信息。这会造成严重故障。

错误辨识和防止

OpenSAFETY 的一项关键机制是时间戳，它可以防止数据重复、混淆和延迟。每个数据包

都被标记以当前时间，使接收端可以避免读重数据，并判断时序和延迟。
OpenSAFETY 不依靠分布时钟，而是通过一个特殊方法为所有节点进行同步。同时采用时间监视方式防止因数据丢失或过长延迟导致的错误，即实时、连续地监视节点。
另外，从提示信息中用户可以知道数据链路层的连接状态。OpenSAFETY 使用 “看门狗”这样一种软件上的机制。在接收端，标识符可以排除一切混淆：OpenSAFETY 帧有一个独特的 8 位或 16 位 ID 标识，包含地址域信息、报文类型和帧类型的信息。最可靠的辨明原始信息发生变化的方法是通过 CRC。它通过一个 key 为每组数据生产校验和，连同 key 本身以位序列的形式加入数据组中。该校验和本身可以看作数据的一个独特的编码。通过位序列和 key，接收端可以计算出原始数据组，并与实际接受到的数据比较。如果检查出任何不同，该条信息就会被忽略。

OpenSAFETY 的帧结构

OpenSAFETY 复制要传输的帧，然后将它们联合为 1 个 OpenSAFETY 帧。因此，OpenSAFETY 帧包含两个有着相同内容的子帧。
每个子帧都有一个独立的校验和作为保障。接收端比较两个子帧的内容。这样的两个子帧中相同数据被改变或破坏的可能性是极低的，并且帧长度增加会让它进一步降低。假使发生最极端的特例，校验和也会起到纠正作用。OpenSAFETY 的这种特殊格式，即两个相同子帧、每个带有独自的校验和的形式，同样使“伪装”也不会出现，排除伪装的标准信息的可能性。

OpenSAFETY 网络

一个 OpenSAFETY 网络可以包含多达 1023 个安全域，每个域又可以包含 1023 个节点或设备。安全域可以跨越不同网络，并且可以将分散在不同网络上的安全节点整合为一个域。安全和非安全谁被可以共处于一个域。通过网关可以使不同安全域之间的通信成为可能。通过 OpenSAFETY，用户可以强制按层级式划分网络，也可以建立各自独立的安全域。比如，可以建立这样的网络：一个域内实施安装，而另一个域中的生产毫不受影响地进行。每个域中，有一个安全配置管理器（SCM）负责连续监视所有安全节点。

适用于通信周期在微秒级的，可以满足达到 IEC61508 的 SIL3（safety integrity level）。它使用几种不同保障机制。除了使用 CRC 监测数据内容，还有一个独立于（非安全向的）传输协议的基于时间的监测。openSAFETY 仅仅用非安全传输层交换安全 openSAFETY 帧，这些帧不会被传输层翻译表达。使用 POWERLINK 与 openSAFETY 在通讯机制上有更密切的联系，因此用 POWERLINK 作为传输协议是最优的。

- 最大 1023 个节点，每个节点 1023 个设备。
- openSAFETY 可以横跨多个/不同类的网络。
- 不同 openSAFETY 域之间的通信通过一个特殊的“openSAFETY 域网关”实现。
- 每个 openSAFETY 域里除了安全节点（SN），还有一个安全配置管理器（SCM），用以分配节点地址，存储节点相关信息，监视安全节点。
- OpenSAFETY 使用与 POWERLINK, CANopen 相似的基础通信机制。（SPDO，SSDO，SOD 等）

综上，介绍了 POWERLINK 具有哪些功能，能解决哪些问题，以及性能指标。这些决定了 POWERLINK 可以用于哪些场合，适合哪种应用。依据 POWERLINK 十几年的使用经验，可以说 POWERLINK 能满足几乎所有的应用的需求。如果对 POWERLINK 的理解很精通，就可以灵活的使用 POWERLINK 的这些功能。对于一些特殊的要求，可能 POWERLINK 现有的功能无法满足，可以通过适当修改 POWERLINK 的代码来满足。