硬实时以太网 ARTC 可靠性保障技术研究*)

陈 慧 熊光泽 罗克露

(电子科技大学计算机科学与工程学院 成都610054)

摘 要 实时网络的很大一部分应用在现场总线控制领域,提供实时、快速、可靠的信息传递。基于以太网的硬实时通信技术 ARTC 能较好地满足工业控制系统实时、快速的通信要求,但以太网的通信特性却导致其缺乏可靠性。本文简要介绍了 ARTC 的通信管理机制,在对其可靠性问题深入研究的基础上,从系统结构、多级自检、监控管理、故障处理以及流控等方面提出了相应的处理策略,能全面提升系统的可靠性,为 ARTC 在现场总线控制领域的应用奠定了坚实的基础。

关键词 实时通信,ARTC,可靠性,双冗余,自检

The Research of Reliability Guarantee Technique over Hard Real-Time Ethernet: ARTC

CHEN Hui XIONG Guang-Ze LUO Ke-Lu

(Computer Science and Engineering College, University of Electronic Science and Technology of China, Chengdu 610054)

Abstract Real-time network is mostly used in the field-bus control domain to provide real-time, quick, reliable messages transmission. The hard real-time communication technology ARTC, based on Ethernet, can gracefully satisfy the request of real-time and quick communication of industry control system. However, it is short of perfect reliability because of the transmission characteristic of Ethernet. In this paper, the mechanism of communication and management in ARTC is presented in brief. Through researching its reliability problems deeply, we present the corresponding policies and the measures of system architecture, multilevel self-test, monitoring and management, failure treatment, flow control, etc. These techniques can enhance the reliability of the system entirely, and establish firmly basic for ARTC application in the field-bus control domain.

Keywords Real-time communication, ARTC, Reliability, Dual-redundance, Self-test

1. 概述

由于微处理器及其相关技术的不断发展,以及现代工业控制系统的广泛应用,用户对现场总线控制系统(FCS)的带宽、传输距离、可靠性和性价比的要求越来越高。以太网(Ethernet)具有快速、协议简单、便宜和兼容性好等特点,但因其所采用的随机争用介质方式和二进制指数回退机制使得 Ethernet 不具有实时性,加上抗干扰能力和可靠性较差,一直以来仅在工业控制网的上层使用。采用交换技术和全双工接驳后,以太网冲突可能性被大大降低,于是人们自然想到将以太网向现场总线底层延伸。但是以太网的非确定性并没有完全得到解决,依然无法应用在具有严格时间限制的分布式控制领域。为此,我们结合现场总线应用特点,提出并实现了一种具有完整体系结构并支持分布式控制的硬实时以太网通信技术 ARTC(Advanced Real-Time Communication)[1]。

ARTC 采用命令/响应多路传输和总线表方式分配底层的总线带宽,其总线使用权完全由主控站控制。ARTC 具备对网络节点的管理能力,支持基本终端在线加入和退出;拥有健全的 CMIB(通信管理信息库)、地址分配和管理机制;能自动生成总线调度表;提供的 ARTC 服务层为用户提供了一个简便、快捷的应用接口。但由于以太网固有的通信特性导致了 ARTC 缺乏可靠性,在条件恶劣的工业现场应用中显得较为脆弱。本文将针对这一问题,详细介绍 ARTC 在系统结构、多级自检、监控和管理、网络故障处理、流控等方面,为全面提升系统的可靠性和容错能力所进行的设计和改进。

以太网逻辑上呈总线型,物理上可采用多种连接方式,ARTC 中采用星型连接方式,各网络节点通过集线器相连。为进一步提高系统的可靠性,我们使用双冗余的接口、线路和集线器(hub),并提供一个监控站作为备份的主控站,逻辑结构如图1所示。

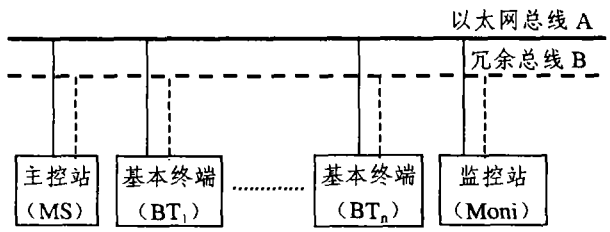


图1 双冗余 ARTC 网络模型

所有网络节点分别经两个独立的以太网接口与总线 A、B 相连,系统中只有一个主控站(MS),也只有一个监控站(Moni),其余为基本终端(BT)。主控站的主要功能则是启动消息和管理总线事务。系统初始化后,MS 指定一条总线为主总线,另一条则作为备份总线,总线使用权由 MS 控制,确保

*)四川省科技厅重点科技项目基金资助(02GG006-037)。陈 慧 博士研究生,主要研究方向为实时通信技术与应用。熊光泽 博士生导师,主要研究方向为实时计算系统及应用。罗克露 教授,主要研究方向为实时系统和 CAD、CI 技术。

在任一时刻仅有一条总线获得使用。正常情况下系统使用主总线通信，当与消息通信相关的主总线设备发生故障时使用备份主线，一旦主总线故障排除，则重新使用主总线通信。MS通过BT(s)的应答信息获知网络节点及设备的状态，确定总线调度表中下一条消息使用的传输线路，BT只需使用与收到所收命令相一致的接口和线路传送数据和应答信息。为支持上述机制的实现，系统初始化时MS为每个节点分配了一个由5bits的MS逻辑ID加上8bits的节点代码组成的网络地址，当所有在线节点地址分配完成后，MS将广播网络节点活动表，表中记录了所有在线节点的网络地址以及与两条总线相对应的物理地址。

监控站(Moni)是系统中指定接收且记录总线上传输的信息，并有选择地提取信息以备后用的终端。同时Moni还具备冗余主控站的功能，当收到主控站在线接管命令或发现主控站故障时均可升级成为新的主控站。

以太网提供了多种传输介质供用户选用，虽然ARTC与设备无关，但为适用于现场应用的恶劣环境，建议选用屏蔽双绞线或光纤。比较而言，光纤的抗干扰能力较强，但带来的开销也更大，用户可根据具体情况选取。

2. 多级自检及主控站管理

为便于网络管理以及双冗余结构的正确应用，系统具备初始化及运行过程中节点软件、节点硬件、网络线路以及整条总线的多级自检能力。在我们提供的硬件板卡上，集成了两块以太网卡芯片且分别与两条总线相连，节点具有对这两块芯片独立的自检能力以及整块板卡的自检能力。网络节点将在其应答帧中捎带自检信息，主控站也可通过消息专门查询。对于近期通信正常的节点，主控站只需按照总线调度表中安排的周期性探测消息进行查询；而对于出现异常的节点，主控站还会产生非周期消息对其进行查询。

ARTC中，当BT收到一个数据帧或命令帧时都会向MS发送应答帧，因此如果节点经自检发现冗余接口故障，该节点将在其应答帧中说明；如果节点的当前接口故障，虽然无法收到和传出消息，然而当主控站从另一总线查询时便能获知其信息；而且在节点的监控模块中存放有该节点软、硬件的自检记录，用户通过本节点管理窗口可获知节点存在的具体问题并采取相应措施处理。由此，既使系统具备对节点的在线管理能力又为用户的事后维护提供了便捷的途径。另一方面，主控站通过周期性的消息查询可分辩出网络上某段链路及整条总线的故障情况。如果网络上某个节点的A接口对查询无应答，而经另一接口返回的信息表示该节点的所有接口均正常，则说明该节点A接口与A集线器间存在链路故障；如果所有节点对经A总线的查询均无应答，而主控站与该总线的接口经自检无误，则说明或者是主控站与A集线器间的链路故障或者是A集线器故障。

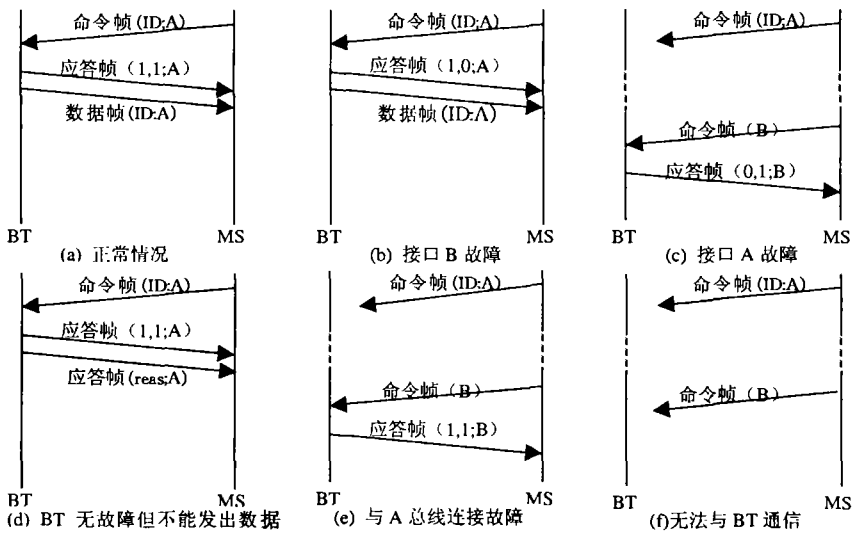


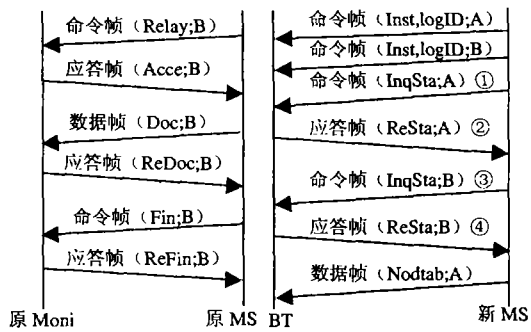
图2 自检及故障信息获取示例

假定主控站与A、B总线间的连接均正常，以从某一基本终端BT到MS的一条数据传输消息为例，图2说明了不同情况下BT自检信息的反馈以及主控站的查询判断。一条从BT到MS完整的数据传输消息由以下帧序列组成：MS到BT的命令帧、BT到MS的应答帧以及BT到MS的数据帧。与该消息传输相关的所有设备和接口均正常情况下的消息传输如图2(a)所示：首先MS经主总线A通过命令帧(ID;A)命令BT向MS传送序号为ID的数据；BT一旦收到该命令，立即经A总线通过应答帧(1,1;A)向MS报告命令帧已收到并捎带其自检信息，其中(1,1)表示A、B接口的自检情况，正常置1，故障置0；接着BT经A总线通过数据帧(ID;A)向MS传送指定序号数据。如果BT自检发现接口B故障，则将应答帧中的相应位置0，如图2(b)所示。图2(c)是BT的接口A故障的情况，此时BT将无法收到从MS发出的命令帧，由于MS没有收到相应的应答帧和数据帧，于是产生一个非周期查询消息插入到总线表的非周期消息时段，BT收到从总线B传来的查询命令立即发出相应的自检应答。而如果BT由于忙或数据未就绪，无法在规定的时间中传出数据，其情况则如图2(d)所示，此时它必须在规定时间到来前向MS发出应答帧(reas;A)说明原因。如图2(e)，假如BT接口均无故障，但BT与A总线集线器之间的连接故障，MS处理与接口A故障时的情况类似，当其收到应答帧后便能分析出上次消息传输夭折的原因。如图2(f)表示MS无法和BT通信，此时MS无论从A总线还是B总线都无法收到BT的应答，通常情况下这是由于BT掉电等原因所致。MS对ARTC的其它几类消息在各种情况的处理判断方式可由此推出，在此不再赘述。由上可见，MS通过对节点的查询以及应答帧信息的分析，便能判断出网络上的故障情况，指导其管理控制。

主控站拥有使用两条总线的控制权，在执行下一条消息调度前，主控站将查询所记录的网络情况，确定这一消息所用线路，并优先使用主总线。仅当参与通信的所有设备均具备某一线路的通信能力时才启动该消息，否则该消息传输时间空闲。各基本终端只简单地记录收到信息的线路，并从相同接口发送其应答信息或数据信息。即，所有节点的所有接口始终处于活动状态收发信息。

3. 主控站移交及监控站接替

在 ARTC 原型系统中，主控站和监控站使用具有较强功能的工控机或 PC 机，而所有的基本终端都使用基于 Intel 386的嵌入式现场设备。监控站仅接收且记录总线上传输的所有信息，并按事先设定的方式有选择地提取信息，主控站将定期对其进行查询，获取这些统计、分析数据。所有网络管理信息仅由主控站上传到上一级管理层，管理员也可使用主控站的人机界面或监控站的管理界面直接查询。除非监控站升级为新的主控站，否则不上传信息。



(a)主控站在线移交过程　(b)新主控站控制处理过程

图3　主控站在线移交及控制过程

监控站除具备对网络传输信息的统计分析功能外，还具备冗余主控站的功能。当监控站收到主控站的接替命令，或确认主控站故障（指主控站与两条总线连接均故障）时监控站将升级为新的主控站。在下述两种情况下主控站有权向监控站发送在线接替命令：一是主控站经自检发现本节点的某个接口故障（如 A 接口）；二是在主控站的最近一次查询中，所有的节点对某条总线（如 A 总线）查询均无应答，这或者是由于主控站与 A 集线器之间的连接故障或者是由于 A 集线器故障。当监控站收到主控站的在线接替命令时使用主控站在线移交的方式[1]升级为新的主控站，其过程如下（见图3(a)）：主控站首先查询网络节点信息表，确认监控站在最近的一次查询中 A、B 接口以及 B 总线连接均无故障；于是主控站通过 B 总线向监控站发送在线接替命令（Relay;B），监控站收到主控站的命令后向主控站返回同意成为主控站的应答（Acce;B）；主控站收到监控站的同意信息，随即向监控站在线传递网络节点活动表和总线调度表等相关文件（Doc;B），监控站收到后通过应答帧（ReDoc;B）确认收到上述文件；最后主控站通过命令帧（Fin;B）通知监控站在线交接完毕，监控站仍需返回对该信息的确认（ReFin;B）；此时原监控站升级为新的主控站，原主控站收到该确认则自动降级为新的监控站。在上述移交过程中，如果因各种原因导致在线移交无法完成，监控站将确认主控站是否故障，并采用主控站故障情况下的方式升级为新的主控站。在线移交完成后新主控站控制处理如图3(b)所示。为能正确调度消息和管理总线事务，新主控站将通过命令帧（Inst，logID；A）和（Inst，logID；B）经 A、B 总线向所有的网络节点广播更换主控站命令同时公布其5bits 逻辑 ID 号，各节点收到该命令将更改其节点地址的前5位，而节点代码则无需重新分配。新主控站接着从两条总线逐一查询各网络节点的状态（见图3(b)中①、②、③、④），并广播网络节点活动表（Nodtab；A），进而调度消息传输。

系统运行过程中，主控站将记录自身的活动情况，在网络空闲时段内主控站会周期性广播其存活信息。监控站的最大等待时间等于主控站活动宣告时间间隔的二倍，如果监控站发现超过最大等待时间网络无活动则认为主控站故障，于是监控站首先通过命令帧向所有网络节点广播，说明原主控站故障，接着初始化网络，广播逻辑 ID 号，收集调度信息，生成总线调度表，查询节点状态，进而调度消息传输。当原主控站故障恢复后，将首先侦听网络活动情况，其侦听时间为监控站的最大等待时间，一旦发现网络上有信息传输，则说明原有监控站已升级为主控站，于是它将激活监控程序模块，作为监控站运行。由于主控站故障及其恢复必定会花费时间，因此网络上不会出现主控站竞争的情况。

只有监控站在两条总线上的传输均正常时，才能进行在线移交或主动升级为主控站。由于主控站记录了节点和链路的最新状态，并定期将这些信息传给监控站，当主控站与一条总线的连接故障时，如果监控站与两条总线中的任意一条存在连接故障，主控站都不能移交其管理控制权，网络将按原有模式运行。仅当监控站发现网络上两条总线均无活动，经自检并查询主控站传来的最近一次状态信息确认本节点通信正常后，才能主动升级为新的主控站。主控站和监控站在各种情况下的处理原则如表1所示。这些原则确保了在同一时刻网络中主控站的唯一性。

表1　主控站移交及监控站升级策略

主控站	监控站	处理原则
A 总线连接故障	无故障	在线移交
B 总线连接故障	无故障	在线移交
A、B 总线连接均故障	无故障	主动升级
A 总线连接故障	A 或 B 总线连接故障	不改变
B 总线连接故障	A 或 B 总线连接故障	不改变
A 或 B 总线连接故障	A、B 总线连接均故障	不改变
A、B 总线连接均故障	A 或 B 总线连接故障	网络瘫痪

4. 站点管理及其它故障处理

主控站在运行过程中将周期性地通过消息查询新节点的加入请求，为其分配网络地址。当在线节点需要退出时，它将通过应答帧向主控站提出请求，得到主控站同意后退出。如果在线节点连续 n 次（n 在网络初始化时设定）无应答，则说明此节点故障，于是主控站删除该节点。当退出节点和被删除节点需要重新参与网络通信时必须按照新节点加入的方式提出请求。主控站会对网络节点的所有上述变动进行广播，以便于各个网络节点修改其 CMIB 库中的节点活动表。

对于各个网络节点来说，其通信表中的每一条数据传输消息都对应着一条相应的数据，总线调度表的排列从理论上确保了在每一条消息的周期（死线）到来之前都能完成传输，同时也保证了该消息被调度时当前周期数据已经就绪。但由于实际网络通信过程中的各种潜在原因依然存在如下两种可能：一是前周期数据尚未传出，后一周期数据却已经就绪；二是网络调度时当前周期数据未能按时就绪。对于第一种情况，一旦后一周期数据就绪，它将无条件地覆盖前一周期数据，以

（下转第85页）

DDoS 入侵检测方法，该方法应用建立正常的网络流量模型、限幅，通过计算网络流量的自相似性(Hurst 参数)的变化，揭示了 DDoS 入侵对网络流量自相似性的影响，提出判断 DDoS 入侵的参数标准，并使用数据库对攻击进行定位。试验表明此方法适合作为检测 DDoS 入侵的依据并且比传统的 DDoS 入侵检测系统在检测的准确度上有较大提高。未来工作是：1、分析多种攻击的各自特点，确定各种不同网络流量异常与正常的临界点；2、我们分析的两种攻击都是流量稳定的，如何确定流量逐渐增大的攻击的特点；3、改进数据库的统计方法以提高检测速度，以便更好地适应实时检测的需要。

参 考 文 献

1 Leland W, Taqqu M, Willinger W, Wilson D. On the Self-Similar Nature of Ethernet Traffic. IEEE/ACM Transactions on Networking, 1994, 2(1): 1～5

2 Popescu A. Traffic Self-Similarity. In: Proc. of the IEEE Intl. Conf. on Telecommunications, Jun. 2001

3 Taqqu M S, Teverovsky V. On Estimating the Intensity of Long-Range Dependence in Finite and Infinite Variance Time Series. preprint Boston University, USA, 1996

4 Taqqu M S, Willinger W, Sherman R. Proof of a Fundamental Result in Self-Similar Traffic Modeling. Computer Communication Review, 1997, 27(2)

5 Meadows C. A formal framework and evaluation method for network denial of service. In: Proc. of the 12th IEEE Computer Security Foundations Workshop, June 1999

6 Willinger W, Taqqu M S, Sherman R, Wilson D V. Self-similarity through High Variability: Statistical Analysis of Ethernet LAN Traffic at the Source Level. IEEE/ACM Transactions on Networking, 1997, 5(1)

7 蔡弘，陈惠民，李衍达. 一种新型的通信网络突发业务建模方法—自相似业务. 通信学报，1997，18(11)：51～59

8 陈惠民，蔡弘，李衍达. 自相似业务：基于多分辨率采样和小波分析的 Hurst 系数估计方法. 电子学报，1998，7

9 Reiher P, Prier G, Michel S, Li J. Project D-WARD: DDoS Network Attack Recognition and Defense', UCLA. http://lever.cs.ucla.edu/ddos/, Aug. 2001

10 Erramilli A, Willinger W, Wang J L. Modeling and Management of Self-Similar Traffic Flows in High-Speed Networks. Network Systems Design, Gordon and Breach Science Publishers, 1999

11 Beran J, Sherman R, Taqqu M, Willinger W. Variable-bit rate video traffic and long-range dependence'. IEEE Trans Commun, 1995, 43: 1566～1579

(上接第74页)

此保证网络上传输的总是最新的数据。对于后一种情况，节点只发送应答帧对该情况进行说明，而不传送数据。另外，系统还对网络节点的响应设置了严格的时间限制，如果节点功能健全却不能在规定时间内发出数据，则该数据不再发出，但必须在该限定时间内发送应答帧并将相应位置1以向主控站说明。

另一方面，应用 ARTC 硬实时通信机制，正常情况下网络不会出现冲突，冲突属于网络通信故障。但是一旦网络发生冲突，按照以太网的冲突回退算法，可能引致网络通信混乱甚至瘫痪。由于现有的以太网芯片普遍支持全双工通信模式，因此通过驱动程序将网卡寄存器的相应位设置为全双工模式，则可屏蔽以太网 CSMA/CD 协议[5,6]。由此，在不改动硬件的前提下，一方面解决了由意外冲突而引发的网络故障问题，另一方面由于屏蔽了载波侦听功能也缩短了硬件发送的响应时间，并为用户使用基于 ARTC 硬实时通信建立支持软实时和非实时的综合网络提供了可能。

5. 流控

在 ARTC 的应用过程中，当数据从发送节点的发送缓冲区通过总线发往接收节点的接收缓冲区时，如果接收节点的接收缓冲区内的旧数据尚未被取走，则可能发生数据覆盖。这是由于发送节点向接收节点发送数据的速率快于接收节点从接收缓冲区中取走数据的速率。

解决数据覆盖一般是引入流量控制，使得发送方发出的数据块流量不超过接收方的接收处理速率。有两类常用的流控方法：反馈流控法和无反馈流控法。反馈流控法指接收方通过某种反馈机制，使发送方通过了解接收方的接收处理能力调节其发送速率，常用的等-停协议、滑动窗口协议都属于这一类。这类方法在解决非实时网络流控问题方面被证明是非常有效的，却较难保证网络数据实时传输，因而不太适用于实时网络。无反馈流控法指接收方按一固定的速率接收数据，发送方通过控制发送速率，使其始终不超过接收速率。这类方法在解决了流控问题的同时也较好地保证了数据的实时传输，不足之处是实现较为麻烦，需要全局考虑，要在满足整个系统的实时性前提下，对收发速率精确计算和设置。

ARTC 采用无反馈流控法避免出现接受方数据覆盖。每个节点都有一个接收任务按一定的时间间隔周期性地查询并移走接收缓冲区的数据，如果这一时间间隔设置过大，则可能导致接收缓冲区覆盖，而如果设置过小则会浪费 CPU 资源，并可能引起其它系统任务的阻塞，因此其关键就在于合理地设置节点的接收任务运行周期。实时系统中消息被分为周期消息和非周期消息，节点的发送速率受总线调度表控制。对于周期消息来说，其在总线调度表中获得调度的时间间隔是确定的，即等于其周期，只要接收任务的运行周期小于消息的周期就不会出现接收方数据覆盖[3]。由于在 ARTC 消息调度过程中所有的非周期消息都被转化成了周期消息，因此我们只需按照周期消息的方式进行处理。现场级应用中，同类终端的工作任务通常是相同的，因此在 ARTC 初始化时，将对每类节点的每一条相关消息分别进行分析，并取其相关消息的最小周期作为接收任务的运行周期，便可解决接收方数据覆盖问题，实现网络的合理流控。

总结 本文从系统结构、多级自检、监控管理、流控以及故障处理等方面，提出了基于以太网的硬实时通信系统 ARTC 系统化的可靠性解决措施，为把 ARTC 应用于现场总线控制领域奠定了坚实的基础。由于现场总线的历史成因以及应用环境存在较大差异，用户对系统的实用性、可靠性、价格以及终端设备属性等的要求不尽相同。因此我们在对 ARTC 系统研究、设计的同时，尽可能地兼顾用户应用中的不同需求，在网络构建、模块设计和终端接入等方面为用户提供足够的灵活性和选择余地。

实时网络的可靠性研究是一个长期而漫长的过程，在实际应用中我们将致力于对上述策略的不断修正和完善。

参 考 文 献

1 陈慧，熊光泽，杨仕平. 基于以太网的硬实时通信技术 ARTC. 计算机科学，2003(7)

2 An Interpretation of MIL-STD-1553B. http://www.1553.com/1553interp.htm

3 王志平，熊光泽，刘锦德. 1553B 实时网络流控问题研究. 计算机科学，1999，26(7)：80～82

4 Tanenbaum A S. Computer Networks. Prentice Hall, 1996

5 Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications. http://standards.ieee.org/

6 Realtek Full-Duplex Ethernet Controller with Plug and Play Function (RealPNP). http://www.realtek.com.tw/