doi:10.3969/j.issn.1671-637X.2013.05.018

综合模块化航电系统高安全性时间管理技术

杜晓鹏， 孙泓宏， 王立端
（中国商飞上海飞机设计研究院，上海 201210）

摘 要：综合模块化航电（IMA）系统中错误信息的传输漏洞会对飞机安全带来严重影响，为了提高IMA系统时间传输的完整性，使子系统能在确定的时间窗口内进行数据传输，提出了一种IMA系统高安全性时间管理技术；通过使用多个时间管理服务，建立每个子系统与时间管理服务的偏差表，确定其本地时间参考（LTR）和与之通信的每个远程子系统时间参考之间的关系；使驻留IMA的子系统具有高安全性时间同步机制，能够协调分离的驻留子系统共同安全地执行同一任务，满足IMA系统时间同步和安全性要求。

关键词：综合模块化航电系统；安全性；时间管理；参考时间
中图分类号：V271.4 **文献标志码**：A **文章编号**：1671-637X(2013)05-0081-04

High-Safety Time Management Technology for Integrated Modular Avionic (IMA) System

DU Xiaopeng, SUN Honghong, WANG Liduan
(Shanghai Aircraft Design and Research Institute, Shanghai 201210, China)

Abstract: False information transmission flaw in Integrated Modular Avionics (IMA) system would seriously impact the aircraft safety. To improve the integrity of IMA system time transmission, a high-safety time management technology for IMA system was put forward, by which all published data on IMA platform will be transferred to subscribers as requested at one designated time window. By using multi-time management service, deviation table between each subsystem and time management service was set up, to identify the relationship between local time reference (LTR) and the time reference of each remote subsystem communicating with LTR. The time management technology provides subsystems hosted in IMA with high-safety time synchronization mechanism, coordinates the separated hosted subsystems to safely execute a task together, thus can satisfy the time synchronization and safety requirements of IMA system.

Key words: Integrated Modular Avionics(IMA); safety; time management; reference time

0 引言

在军用和民用飞机的航电领域中，广泛采用了综合模块化航电（IMA）系统，IMA是灵活的、可重用的开放式系统架构。IMA平台为执行实时功能的驻留应用提供数据计算、数据传输和数据接口功能，在公共平台资源上可以构建多个驻留子系统形成一个高度集成的系统，每个驻留子系统形成隔离和独立的特点。IMA平台提供了健壮分区隔离和其他保护措施，这些措施允许多个应用共享一个平台以及平台上的资源，支持飞机功能在高安全性和容错网络上分布，可以用于支持驻留关键的系统功能[1]。

IMA系统中不同的子系统设备、节点、平台模块或者另外的设备间进行数据交换必须准确以及能够满足飞机功能的完整性需求[2]，IMA系统中错误信息的传输漏洞会对飞机安全带来严重影响，为了满足数据传输的安全性，使IMA平台在一个指定的时间窗口内准确无误地将所有数据传输给所需要的收件方，IMA平台必须能够为各交联系统提供安全的数据传输机制。构建IMA平台的时间管理（NTM）功能，使每个子系统确定其本地时间参考（LTR）和与之通信的每个远程子系统时间参考之间的关系，即用来进行完整的数据传输功能，在时间完整性方面提供失效模式和失效检测，以保证在确定的时间内将数据交付给用户，并降低未

收稿日期：2012-03-20 修回日期：2012-07-12
作者简介：杜晓鹏（1974—），男，山西交城人，硕士，高工，研究方向为航电系统、分布式计算机系统、数据采集系统、自动测试系统。

探测到的错误数据概率,满足灾难等级故障状态分类的功能要求。

1 数据安全性

为了满足飞机的安全性需求,IMA 平台和驻留应用就要满足分配给 IMA 系统的功能完整性与可用性的需求。对于飞机功能和驻留应用,IMA 系统的架构应能支持最高级别的完整性和可用性。

飞机级功能所期望的可用性与完整性等级,平台对其进行支持所需的能力和方法,以及分配到特定 IMA 系统的飞机安全性和信息安全性需求都应得到确定,并要通过 IMA 系统设计来满足,包括指定系统的研制保证级别、硬件及软件的设计保证级别。这些安全性级别的确定要通过飞机级安全性评估来进行[3],从而确定这些级别可以支持由驻留应用实现的功能系统,并支持系统的可用性和完整性需求。

1.1 数据时间完整性

IMA 系统对数据传输的时间完整性需求(消息完整性)是非常复杂的,因为每个子系统都有自己独立的本地时间参考(时钟)。发送数据的子系统必须加入时间戳信息,接收子系统读取时间戳和进行检测[4]。这样,有确定性延时要求的接收子系统,能够知道本地参考时间和发送子系统参考时间的偏差。但是,由于时钟漂移、源系统的时间精度和不同的启动时间等因素,不同子系统时间参考是不同的。

如图 1 所示,子系统 1 发送一条消息给子系统 2。

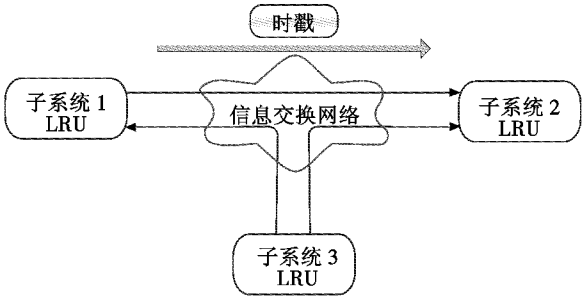

图 1 数据完整性检查

Fig. 1 Integrity check of data

子系统 1 发送消息时,将根据本地参考时间产生一个时间戳,时间戳将包含在发送信息里。从子系统 1 发送到子系统 2 根据不同的传输路径将会出现不同的延时情况,许多因素会造成这种延时问题,例如发送子系统调度延迟、链路速率、交通竞争等。消息到达子系统 2 后,必须使用本地参考时间检查信息延时时间。为了计算信息延时,子系统 2 需要知道本地参考时间和子系统 1 的参考时间之间的偏差,只有在这种情况下,信息端到端的延时情况才能被确定。

1.2 时间完整性的验证

完整性验证就是获取本地系统时间和远程系统时间之间的偏移量,在误差允许条件下计算接收到信息的期龄。将计算的信息期龄与系统设定的阀值比较,如果计算的信息期龄大于设定的阀值,那么这条信息将被丢弃。如果不能确定系统时间偏移量,时间完整性无法验证,只能提供给系统未经时间完整性验证的信息。

2 主时钟时间同步技术

目前,工业控制系统和安全性要求不高的系统经常都采用主时钟时间同步技术进行时间完整性的确认,它的时间同步方案使用了网络测量和控制系统的精密时钟同步协议标准(Precision Time Protocol,PTP)IEEE 1588[2-3]。IEEE 1588 标准的全称是“网络测量和控制系统的精密时钟同步协议标准”,于 2002 年发布,是通用的提升网络系统定时同步能力的规范。它的基本原理是通过一个同步信号周期性地对网络中所有节点的时钟进行校正同步,使分布式系统达到精确同步[4-6]。该协议通过交换报文来确定分布式系统中的主时钟(Master)和从时钟(Slave)之间的时间偏移及报文传输的网络延迟,根据偏差 Δ,调整从时钟,实现对时。处于主时钟状态的设备被认定为精确时钟,它将同步从时钟的时间,但在同一个通信子域内只能存在一个主时钟[7-9]。对于使用 IMA 平台的航电子系统的高安全性需求,数据传输要求带宽是固定的,且传输一条消息所消耗的时间是常量,另外,它需要特殊冗余或源选择技术以满足 IMA 系统的可用性和完整性[10]。因此,本文提出一种可以满足高安全性数据传输要求,时间管理协议简单、易于验证,且传输延时确定的 IMA 系统高安全性时间管理技术。

3 高安全性时间管理技术

高安全性时间管理是为了确保 IMA 系统高完整性和高可用性的数据传输功能,它为驻留 IMA 平台的子系统之间传输数据提供时间完整性检查机制和冗余的时间管理服务。通过构建多个 IMA 系统时间管理服务,为每个子系统启动时配置本地参考时间,建立每个子系统与时间管理服务的时间偏差,并通过故障容错技术向每个子系统分发的时间管理技术来实现 IMA 系统高完整性数据的通信。

3.1 系统参考时钟

系统时钟是由时间管理服务时钟和 IMA 系统的子系统以及交联子系统的时钟构成的一种对等关系的时钟层次结构。每个子系统都有本地物理参考时钟(LCR),同时,需要建立本地逻辑参考时钟(LTR)用于

验证信息的时间完整性和给发送的信息增加时间戳。本地逻辑参考时钟是由本地物理参考时钟来驱动，在整个系统运行期间，提供单调时间增加值，本地逻辑参考时钟在启动时将根据多个时间管理服务发送的时钟信息进行调整。源子系统发送信息的时间戳(STS)和目的子系统时间戳(DTS)将从本地逻辑参考时钟获得。

3.2　时间管理机制

IMA 系统的时间管理机制就是为各子系统周期性提供相关子系统的时间相对偏差值(ROS)和时间相对偏差值误差(ROSE)，用于数据的时间完整性验证。系统的时间管理服务通过从所有子系统采集当地时间参考信息，并在内部形成一个系统时间偏差表，时间管理服务将这个偏差表发送给所有相关子系统。每个接收到偏差表信息的子系统必须从偏移表里选择正确的偏移值配对，也就是它自己的偏移值和发送信息系统的偏移值，然后计算本地参考时间和与自己通信的每一个远端子系统之间的时间偏差量(TOS)，如果在一定的阈值内没有足够的信息计算 TOS 值，那么 TOS 将被认为是无效的。接收子系统根据 TOS 值计算出接收到信息的延时情况。

为满足系统高的可用性需求，需多个时间管理服务用于冗余时间偏差计算。一般来说，为满足支持危险级以上的系统驻留，至少需建立 3 个系统时间管理服务。如图 2 所示，时间管理服务采用时间请求/回复通信机制，每个时间管理服务使用 1 Hz 的频率发出一个时间请求信息给所有子系统，它包括初始同步、偏差表建立和偏差表分发 3 个阶段。

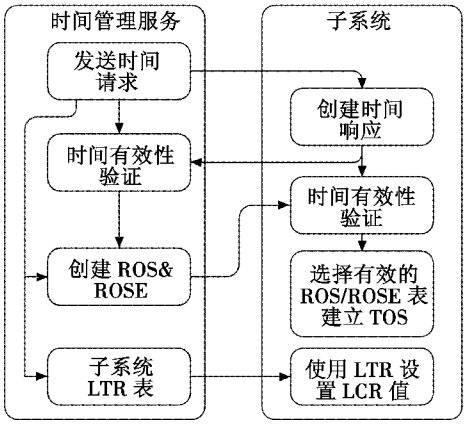

图 2　时间管理机制

Fig. 2　Time management overview

1）初始同步阶段：在初始阶段首先进行时间同步，获得的首次时间参考即同步的起始时间。

2）偏差表建立阶段：根据时间管理服务设定的请求/回复周期(即系统要求同步间隔时间)，周期触发当地时间请求并捕获每个子系统的 LTR，且计算子系统与时间管理服务之间信息往返的时间延时。

3）偏差表分发阶段：时间管理服务按照设定的分发周期，向每个子系统发送时戳列表和时间偏差表。

3.3　时间管理协议

图 3 描述了一个时间管理服务和交联子系统单周期的通讯协议，每个协议按照 2 s 的周期进行循环，每个协议周期包括 4 个 500 ms 的时间片断。

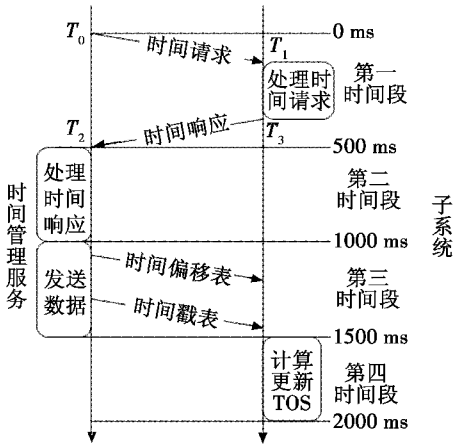

图 3　时间管理协议循环

Fig. 3　Time management protocol cycle

1）第一时间段。时间管理服务首先使用高优先级的通讯服务，在 T_0 时刻向每个子系统发送时间信息的请求，各子系统接收到时间管理服务发送的请求后，将立即记录当前本地时间参考信息，在对时间管理服务发送信息验证正确后，把刚刚记录的时间信息作为 T_1 时刻时戳。子系统处理接收到的时间信息，采集本地时间建立发送时刻时间信息，作为 T_2 时刻时戳，而后即刻创建一个包括 T_1 和 T_2 时戳信息的数据包发送给时间管理服务。

2）第二时间段。时间管理服务接收子系统的时间响应后，也将即刻记录当前本地时间，服务应用对接收到的信息进行验证和处理，建立 T_3 时刻时戳。时间管理服务把 T_3 时戳加载到一个时戳列表，同时时间管理服务根据初始信息请求时刻 T_0、子系统接收时刻 T_1、子系统响应时刻 T_2 和服务接收到的子系统响应时刻 T_3 计算出时间偏差信息，并加载到时间偏移表中。若时间管理服务请求/响应通信没有建立，那么时戳列表中子系统时间偏差配置入口就应设置成无效状态。

3）第三时间段。时间管理服务负责为每个子系统维护时戳列表，以及为整个系统建立时间偏移表，该偏移表内包含 ROS 和 ROSE 的值。时间管理服务向所有交联子系统发布一个时间偏移表和一个时戳列表，所有时间列表将按照定义好的顺序发布。每个交联子系统将在时间管理服务发出时间请求响应后 1500 ms 内接收到 ROS 和 ROSE 信息。

4）第四时间段。每个交联子系统接收到一个时

间偏移表和一个时戳列表后进行验证和处理,并根据远程子系统的 ROS 和 ROSE 信息计算出相应 TOS 值的列表。如果一个远程子系统的 TOS 值在 6 s 内没有刷新,那么就需要设置 TOS 值为无效,同时取消信息期龄的验证。

3.4 时间偏差的计算

时间管理服务功能为每个需传输高完整性数据的交联子系统计算相对时间偏差和相对时间偏差误差值,ROS 表示时间管理服务和交联子系统之间的时间偏差。对于每个交联系统,需计算两个 ROSE 的值:一个是 ROSEA,代表由于系统时钟漂移和标记时间戳引起的绝对误差;另外一个是 ROSEM,表示由于数据传输延时变化引起的最大误差。每个时间管理服务通过时间偏移表向所有交联子系统发布 ROS 和 ROSE 数据,每个交联子系统从时间偏移表选择数据去计算响应 TOS 值,如图 4 所示。

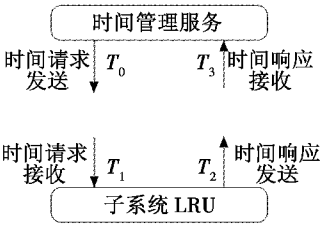

图 4 时间管理协议计算

Fig. 4 Time management computations

ROS、TOS、ROSEA、ROSEM 的计算如下:

$$ROS = T_1 - T_0;$$

$$ROSEM = (T_3 - T_0) - (T_2 - T_1);$$

$$ROSEA = MaxClockDriftLocal + MaxClockDriftRemote;$$

$$TOS = (ROS_{Remote} - ROS_{My}) + (ROSE_{Remote} + ROSE_{My}) + MAX(ROSE_{Remote} + ROSE_{My})。$$

为了满足系统的高可用性需求,每个子系统需处理 3 个时间管理服务发送的时间偏差表信息,即每个有高完整性需求的子系统应该实时监控每个时间管理服务,当某一个时间管理服务故障后,可切换到另外一个时间管理服务。

另外,子系统还需实时测量 T_3 时戳和本地时戳的差异以检测数据是否刷新,以及确认每个子系统计算 TOS 时使用了相同协议周期的时间偏差信息。

3.5 时间参考和模式管理

在飞机系统上电时,时间管理服务将本地时间发送给每个子系统,用于初始化同步,在飞机供电循环,当其他子系统仍然工作时,任何一个子系统都有可能发生重新启动,这样也会造成时间不同步,因此,需子系统启动后调整本地时钟,与时间管理服务时钟同步。

时间管理功能为每个远程子系统维护 LTR 时戳,用于配置高完整性时间数据的传输,每个时间管理服务以 1 Hz 的频率发布时戳列表给每个子系统提供时戳。

正常情况下,每个子系统在系统启动后,将立刻从至少一个时间管理服务接收时间戳列表信息,并根据子系统索引标识更新本地系统时间。系统复位和重启时,如每个子系统还未从时间管理服务接收到 LTR,应禁止任何高完整性数据的传输,直到 LTR 被时间管理服务所更新,并确保相关子系统的 TOS 入口值更新。如果从多个管理服务接收到时间戳列表信息,那么,其中中间数值的时间戳信息将优先用于本地时间的更新。

3.6 安全性

IMA 系统时间同步过程中有可能发生错误,系统时间管理服务和子系统应该具有容错能力,因此需在系统时间管理服务考虑容错算法,对没有及时接收和发送数据、将错误的时间偏移信息发送给子系统,以及没有接收到相同期内的数据进行容错处理。

本方案主要的优点是时间同步和信息传输具有很高的可用性和完整性,使 IMA 系统适应于驻留关键的系统。它可以至少有 3 个时间管理服务运行在不同模块上,周期性地计算和分发时间管理服务与子系统的时间偏差。当一个正在使用的时间管理服务出现瞬态故障和偶发中断,或者丢失几个时间同步信息时,系统能正常地进行时间同步和数据传输。为进一步提高系统时间高完整需求,各子系统可通过对接收到的两个时间管理服务系统时间偏差表进行比对。

4 结束语

时间管理是 IMA 系统与交联系统高完整数据传输的基础。为满足 IMA 系统时间高完整性传输要求,验证交联系统发送来的数据的期龄,通过 IMA 系统高安全性时间管理机制,构建系统时间完整性验证方法。在本方法里,每个子系统知道所有交联系统和时间管理服务的相对时间偏差,信息发起者将所发数据打包上本地时戳发送给相关系统,每个接收子系统根据时间管理服务发送的相对时间偏移表,建立与所有交联子系统时间偏差表,因此能够计算出接收数据延时,保证了子系统的使用关键数据时间差异值限定在系统指定的范围内,同时在系统运行期间进行不间断的时间同步。

参 考 文 献

[1] RTCA Inc. Integrated Modular Avionics (IMA) development guidance and certification considerations [M]. Washington DC: RTCA Inc, 2005.

[2] AC 20-156. Aviation databus assurance[S]. FAA, August 4, 2006.

(下转第 96 页)

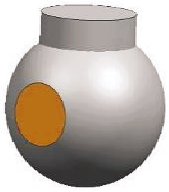

图3 光电系统模型1

Fig. 3 The electro-optical system model 1

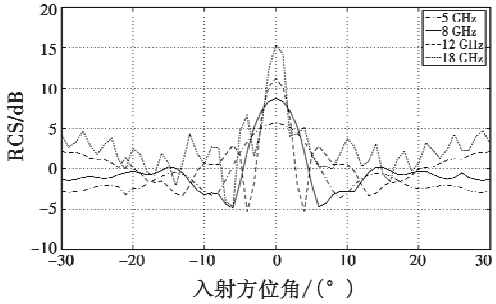

图4 光电系统模型1的RCS计算结果

Fig. 4 The RCS of electro-optical system model 1

图5所示的模型是在图3所示光电系统的基础上,在外部添加了两片倾斜一定角度的平板光窗。平板光窗上采用金属网栅对雷达波进行屏蔽,利用物理光学法对光窗前方方位±30°范围内的雷达散射截面进行了计算,入射波频率取5 GHz、8 GHz、12 GHz和18 GHz,采用垂直极化方式,仿真结果如图6所示。

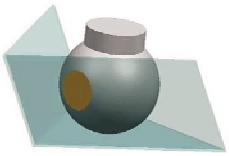

图5 光电系统模型2

Fig. 5 The electro-optical system model 2

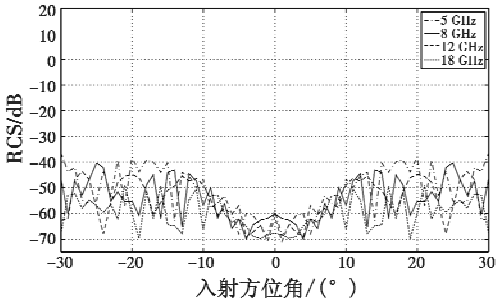

图6 光电系统模型2的RCS计算结果

Fig. 6 The RCS of electro-optical system model 2

4 结论

通过对比仿真结果可以发现,将整个光电系统放置在大片平板隐身光窗之后可以在一定空间方向上有效缩减其雷达散射截面积,提高系统的隐身性能,与上述对国外隐身飞机光电系统的特点分析结果一致。

参考文献

[1] 李保中,韩邦杰,李艳晓. 光电系统半实物仿真系统技术概述[J]. 电光与控制,2010,17(4):30-33.

[2] 赵妙娟,张红刚. 国外机载光电系统隐身技术综述[C]//火力与指挥控制2007年学术年会论文集,2007:6-8.

[3] Jane's Electro-optical system[Z]. 2008-2009.

[4] MOIR I, SEABRIDGE A, JUKES M. Military Avionics Systems[M]. John Wiley & Sons,2006.

[5] 刘敬民,王浩,张洁. 先进战斗机光电综合系统发展综述[J]. 光电技术应用,2007,22(6):4-6,19.

[6] 钱缨,滕祥红,杜洪兵,等. 具有雷达波隐身功能的红外窗口的研制[J]. 人工晶体学报,2008,37(5):1162-1165.

(上接第84页)

[3] SAE ARP4754A-2010. Guidelines for development of civil aircraft and systems[S]. SEA, 2010:32-35.

[4] 叶卫东,张润东. IEEE 1588精密时钟同步协议2.0版本浅析[J]. 测控技术,2010(2):1-4.

[5] 李聪,高丽. 基于IEEE 1588的时钟同步技术在分布式系统中的应用[J]. 电子设计工程,2009,17(12):54-56.

[6] 孔令彬,文赫胜,陈向文. IEEE1588精密时钟同步关键技术研究[J]. 计算机测量与控制,2010,18(7):1585-1588.

[7] 戴宝峰,崔少辉,王岩. 基于IEEE 1588协议的时间戳的生成与分析[J]. 仪表技术,2007,36(7):15-17.

[8] 同江,蔡远文,解维奇,等. IEEE1588精确时钟同步技术[J]. 导弹与航天运载技术,2010(4):37-40.

[9] 程春姬. 综合模块化航电系统时间管理技术[J]. 航空电子技术,2010,41(1):17-21.

[10] NATO. Modular and open avionics architectures part VI-Guidelines for system issues Vol. 5: Time management [S]. ASAAC, 2005.