doi:10.3969/j.issn.1671-637X.2015.06.017

CCAR23部飞机航空电子网络中FlexRay协议的设计和实现

刘 绚, 孔德岐, 张 双, 李 莉, 缪伟涛, 刘文学
(中国航空工业集团公司西安航空计算技术研究所,西安 710068)

摘 要: 为了增强FlexRay网络在CCAR23部飞机航空网络应用中的安全性,分析了FlexRay协议的传输特性,定义了心跳消息结构,提出了在静态段中进行状态声明、在动态段中进行成员协商以及在网络空闲时间进行成员状态决策的成员算法的设计与实现。该算法以进程为单位进行管理,可以在协议层实现进程的重新集成,且对于存在n个故障的系统,只要系统中存在$2n+1$个过程且$n+1$个过程运行正常,该算法就能够在一个周期内识别全部故障。经应用验证,该算法能够在一个通信周期中实现成员协议要求的确认性、一致性以及自我诊断性。

关键词: CCAR23; 航空电子系统; FlexRay协议; 成员协议; 容错
中图分类号: V271.4 **文献标志码**: A **文章编号**: 1671-637X(2015)06-0073-04

FlexRay Protocol Design and Realization in Avionic Network for Aircraft Complied with CCAR23

LIU Xuan, KONG De-qi, ZHANG Shuang, LI Li, MIAO Wei-tao, LIU Wen-xue
(Aeronautical Computing Technique Research Institute, AVIC, Xi'an 710068, China)

Abstract: In order to enhance the safety of FlexRay protocol applied in avionic network in aircraft complied with CCAR23, a heartbeat message structure is defined and a membership protocol algorithm is designed and implemented for FlexRay protocol based on its transmission characteristics. The algorithm consists three phases: status announcement in static segment, negotiation in dynamic segment and decision-making in network idle time. It uses processes hosted by the node as management target and enable the reintegration of a process. Within one cycle, it can identify n faults in a $2n+1$ processes member group while at least $n+1$ process are without fault. Test result shows that the algorithm satisfies the validity, agreement and self-diagnosis requirements of membership protocol.

Key words: CCAR23; avionic system; FlexRay protocol; membership protocol; fault-tolerance

0 引言

在我国加快CCAR23部飞机发展的情况下,FlexRay网络作为具有时间触发特性的分布式实时网络架构,其固有的时间确定性以及传输速率,灵活性和价格等方面的总体性能高于其他总线,使之能够更好地满足CCAR23部飞机中航空电子系统通信的需求。经过测试证明,FlexRay总线的软件性能特征适合作为航空电子局部总线[1],但是FlexRay协议对于成员协议的缺失[2],降低了其在故障检测和控制、平稳降级运行以及冗余管理方面的能力,降低了应用FlexRay协议的系统的安全性[3]。现有针对FlexRay协议设计的成员协议或以节点为监控对象[4],或需要两个通信周期完成故障确认[5],故障确认的效率较低。

本文给出了以CCAR23部飞机航空电子系统网络为应用目标,以进程为管理对象,可在单周期内识别故障的FlexRay成员算法,可以提高故障检测效率。

1 FlexRay协议介绍

FlexRay的通信周期组成见图1。其中,静态段用于进行时间触发通信,采用静态时分多路访问进行传输仲裁;动态段进行事件触发通信,采用基于mini-slot的动态模式进行传输仲裁。Symbol window (SYM)用于进行测试,是通信周期中的可选组成。Network idle time是通信周期中必须包含的内容,可用于进行时钟同步和网络管理。

收稿日期:2014-10-09 修回日期:2014-10-29
作者简介:刘 绚(1982—),女,陕西西安人,硕士,工程师,研究方向为航空电子设备与系统。

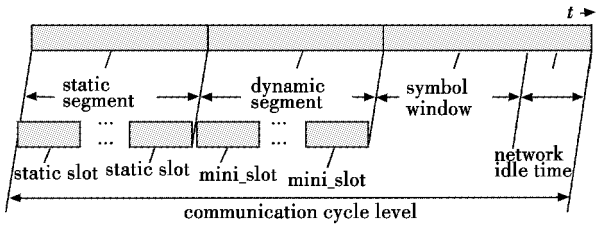

图1 FlexRay 通信周期组成

Fig. 1 Timing hierarchy within the FlexRay communication cycle

2 成员协议

成员协议用于分布式实时系统中,供一组协作的过程之间建立起关于其他过程的运行状态的一致性视图。通过成员协议可以增加分布式过程之间的协作关系,为系统的容错、平稳降级运行以及冗余管理提供支持。成员协议具有以下需求[5-6]。

1) 确认性。在任意时间,无故障过程的成员向量中应包含且只包含所有无故障过程。但是由于对故障进程的诊断需要时间,因此这条需求是难以满足的。因此在实现时,根据采用的成员协议算法,会对这条需求进行适当更改。

2) 一致性。所有的无故障过程应包含同样的成员组成。

3) 自我诊断。故障节点应最终诊断出自身的故障,并在自己的成员向量中表明自己处于故障的状态。

3 CCAR23 部飞机航空电子系统中 FlexRay 成员协议的设计

3.1 成员组定义

如图2所示,在FlexRay网络上可以连接 $m(0<m\leqslant 64)$ 个节点,每个节点上运行不同个数的进程。同一节点上的进程间分区运行,即彼此间故障隔离,不同的进程彼此之间又相互协作完成特定的任务,成员组定义为一组相互协作的进程的集合,成员协议在成员组中运行。本算法所使用的系统模型定义见图2。

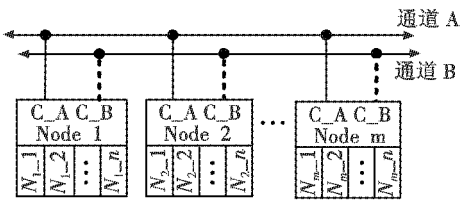

图2 系统模型定义

Fig. 2 System model definition

3.2 成员协议运行机制

FlexRay 协议中的成员协议的运行分为3个阶段。

1) 状态声明阶段。在静态段中,各个过程通过心跳消息将自己的运行状态在网络上进行广播,接收节点将接收到的心跳消息和本地维持的该过程的状态进行比较,如果一致,则不做修改,如果不一致,则进行状态修改,并标记。

2) 成员协商阶段。在动态段中,各个过程将自己维持的成员向量在网络上进行广播,接收节点对接收到的成员向量中各个成员的状态进行标记。

3) 成员状态决策阶段。在NIT段中,各个节点对自己维持的成员向量的标记按照决策算法进行修改。

3.3 心跳消息定义

对 FlexRay 的帧中的有效数据段做如下约束:Data0 和 Data1 用于传输心跳消息。对 Data0 的位定义如下所述。

1) 0~1 位(HBFlag):标示是否包含心跳状态标识的标志。

2) 2~3 位(state):过程状态标识 HB,标示过程运行的3种状态,即正常、需要退出成员组、过程运行正常但当前不在成员组中。

3) 4~7 位(JMFlag):过程措施标识,包含过程的运行故障信息,或申请加入成员组,或希望重新进行成员协商。

3.4 成员协议算法设计

根据3.2节中定义的3个阶段,在包含心跳标识的情况下,算法分别描述如下。

1) 状态声明阶段。

状态声明阶段算法中包括如下关键定义:

① Bool ReceiveFlagK,描述是否接收到有效的心跳消息,它由 FlexRay 协议中的帧有效性标识 vSS! ValidFrame 及消息中 HB 标识和本地维护的对应过程状态的状态比值决定;

② localHBM 定义为本地过程的心跳消息;

③ revHBM 为接收到的心跳消息;

④ MemP[slot]为本地维持的成员向量中在 slot 发送的过程的成员状态;

⑤ slot 代表当前 slot 中发送过程的 ID。

```
对于任意过程 p
If(p! = slot) // 过程 p 是接收消息过程
{
  Receive();
  If(ReceiveFlagk = = FALSE)//未接收到来自过程 k 的心跳消息或心跳消息显示过程 k 退出成员组
  {
    localHBM -> JMFlag = 0011;//需要进行协商
    localHBM -> r = slot;
    MemP[slot] -> state = 00;//成员向量显示为故障
  }
  else if (revHBM -> JMFlag = = 0011)//接收到的心跳消息,其中表明需要进行更改
```

```
  {
    If((localHBM->JMFlag ==0011)
      && localHBM->r==revHBM->r) //表示在本过程发送过协商申请之前已经有其他进程发送出来
    {
      localHBM->JMFlag =0000;//撤销需要协商标识
      localHBM->r=NULL;
    }
  )
  else if(revHBM->JMFlag ==1111)//重新加入申请
  {
  Mem_p[revHBM->slot ]-> state==11;
  }
  else //接收正常
  {
    Mem_p[revHBM->slot ]->state=TRUE;//成员向量显示为正常
  }
}
else//p 为发送消息过程
{
  If(ReIntegration==TRUE)
  {
    localHBM->JMFlag =1111;
  }
  Send(HBMp)//发送过程 p 的心跳消息
  localHBM->JMFlag =0000;//需要进行协商
  localHBM->r=NULL;

}
If((slot==lastSlot) && (p==1))
  Send(HBM1)//过程 1 的心跳在一个周期中发送 2 次,以校对最后一个过程的状态
```

2）成员协商阶段。

在成员协商阶段,每个过程都有机会发送自己的成员意见。成员协商阶段算法中关键定义为:Mem_P[i]->rejMem 表示所有产生拒绝意见的进程的集合,“+”操作表示在该集合中增加元素。

```
While(slot<MAXProc)//在消息发送的各个 slot 中
{
  if(p≠slot) // 过程 p 是接收过程
    {
      for(i=0;i< MAXProc;i++)
      {
        if(ReceiveMem[i] != Mem_p[i])
        {
        Mem_p[i]->rej=Mem_p[i]->rej+1;
        Mem_p[i]->rejMem=Mem_p[i]->rejMem ∪{slot}
        }
        else
        {
          Mem_p[i]->accpt=Mem_p[i]->accpt+1;
          Mem_p[i]->acceptMem=Mem_p[i]->accpMemt∪{slot};
        }
      }
  }
  If(p==slot)// 过程 p 是发送过程
    Send(Mem_p);
}
```

3）成员状态决策阶段。

决策阶段算法中关键定义:Integer$K$ 为系统预先配置的成员有效判定阈值。成员的状态采用 K 个以上成员所达成一致的状态。K 的设置由系统集成商根据任务所涉及到的过程的个数 n 决定,要求 $K\geqslant[n/2]+1$。

```
for(i=0;i<n;i++)
{
  If(Mem_p[i]->accpt>K)   //K 为判定阈值
  {
      Mem_p[i]->state=Mem_p[i]->state;
      for(j=0;
j<getNum(Mem_p[i]->rejMem);j++)
      Mem[Mem_p[i]->rejMem[j]=00;//所有产生少数意见的进程都认为是故障进程
    }
  else
    {
    Mem_p[i]->state != Mem_p[i]->state;
    for(j=0;
j<getNum(Mem_p[i]->rejMem);j++)
    Mem[Mem_p[i]->acceptMem[j]]=00;//所有产生少数意见的进程都认为是故障进程
  }
}
```

3.5　成员协议算法分析

根据 ARP4761[7]对故障的定义,即故障为组件或系统内不希望出现的异常状态,可做出以下推断:任何故障必定能够对系统产生影响。同时引用 TTP 协议中的故障假设作为 FlexRay 网络中的故障假设。

Assupmtion1:系统中存在发送故障和接收故障。另外,还需要一个假设,即 Assumption2:在任意时刻,系统中出现故障的进程总属于少数派。

在此基础上将针对发送故障和接收故障分别对本算法进行分析。

3.5.1　发送故障分析

发送故障仅在发送节点上出现。因此,当 p 为发送节点且出现发送故障时,根据 Assumption2,系统中不再出现其他故障,因此在状态声明阶段,其他节点将不能收到节点 p 的工作正常报告,因此,p 将从正常节点的成员组中被剔除,但是,p 中仍包含其自身。经过成员协商阶段的协商,p 属于少数派,因此在决策节点

可以认定出现故障,将自身从成员组中剔除。

3.5.2 接收故障分析

接收节点 p 接收来自发送节点 r 的心跳信息时出现故障,但是不能判定为 r 的发送故障还是 p 的接收故障,因此 p 对此状态做出标识,并更改 r 的状态为故障。

若 p 为 r 之后的发送节点,则 p 会发出因为 r 而需要进行更改的要求。其他成员接收到该状态后,和本地的 r 状态进行对比,如果和本地的 r 状态一致,则确认 r 为故障;如果不一致,则更改 p 的状态为故障。p 属于少数派,因此在决策节点可以认定出现故障,将自身从成员组中剔除。

若 p 为 r 之前的发送节点,当 p 出现接收故障时,则在协商阶段,p 属于少数派,因此在决策节点可以认定出现故障,将自身从成员组中剔除。

3.5.3 算法效率分析

假设在 n 个过程的系统中,最优情况是没有故障发生,最差情况是存在故障发生,执行最长程序序列。最差情况下,单个节点上的算法时间开销为

$$T_1 = nt + nO(n) + O(n^2) \quad (1)$$

式中:t 为状态声明阶段算法执行单次的固定时间开销;$O(n)$为成员协商阶段算法的开销;$O(n^2)$为成员决策阶段算法的开销。

该算法在网络中传输的时间开销与系统的配置关系密切。如果一个系统,在任何一个周期中,每个节点都需要发送消息,则心跳消息以及成员向量可以和节点消息在一个帧中发送。此时,不需要增加额外的传输时隙,但是仍会增加系统的传输载荷,而网络空闲时间中成员状态决策所需的时间不变。

在最差情况下,系统中每个节点占用独立的时隙发送成员算法相关消息,则执行该算法会给网络带来的额外时间开销为

$$T_2 = n(T_{SS} + T_{DS}) + O(n^2) \quad (2)$$

式中:T_{SS}为静态 slot 的长度;T_{DS}为动态 slot 的长度。

3.5.4 结论

根据以上分析可以看出:在一个决策过程结束后,无故障过程的成员变量中不包含单一的故障过程,故障过程可以识别出自身的故障并退出成员组。因此,该成员协议可以实现成员协议的确认性、一致性和自我诊断性特征要求。

为识别系统中 n 个故障,系统中至少需要 $2n+1$ 个过程,且 $n+1$ 个过程运行正常。

在进程数为 n 的网络实现中,该算法在应用过程中占用的传输时间为 n 个静态 slot 的长度和 n 个动态 slot 的长度以及网络空闲时间中的决策时间。

4 应用实例

采用 10 Mbit/s 的 FlexRay 网络互连起来的航电设备如图 3 所示。该实现中,单独的时隙传输成员协议,每通信周期时长 200 ms,每个静态 slot 时长 15 ms。这是一个简化版的实现方式,即每个节点只有一个过程。

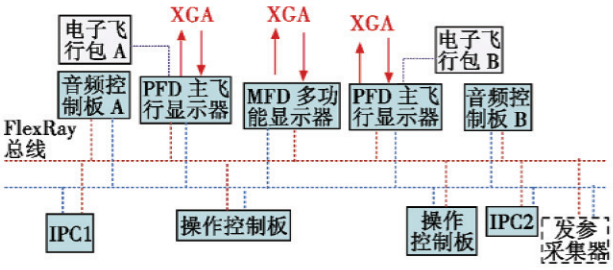

图 3 FlexRay 网络实现

Fig. 3 Implemenation of FlexRay network

应用设置在一个由 5 个过程组成的成员组中,其成员按照发送顺序依次为 P1,P2,P3,P4,P5。令 P2 在 P5 发送前出现一次偶发的接收故障,判定阈值 $K=3$。经过运行该算法,在决策阶段结束时,P2 的故障可以被所有进程识别,并退出成员组。

测试结果表明,增加的网络负载为 475 Byte/s。成员状态决策所需时间小于 1 ms。

5 结语

本文描述了 FlexRay 协议的成员协议的算法设计及其在 CCAR23 部飞机航空电子系统中的实现。该成员算法利用了 FlexRay 通信周期的特征,分为状态声明、成员协商以及成员状态决策 3 个阶段。该算法能够在一个通信周期内实现成员协议要求的确认性、一致性以及自我诊断性,并且相较于 TTP 中集成的成员协议[8-10],该算法可以进程为单位,在协议层实现进程的重新集成,且对于存在 n 个故障的系统,只要系统中存在 $2n+1$ 个过程且 $n+1$ 个过程运行正常,就能识别全部的故障。

参 考 文 献

[1] VIRAKTAMATH C, PEITZ G, STRAUSS U, et al. Evaluation of software performance characteristics of FlexRay communication protocol for its suitability in avionics[J]. Aerospace and Electronic System Magazine, 2008, 23(9): 4-13.

[2] FlexRay Consortium. FlexRay communications system protocol specification(Version 3.0.1)[M/OL]. [2014-09-03]. http://www.flexray.com, 2006.

(下转第 92 页)

[7] 关新平,范正平,彭海朋,等. 扰动情况下基于 RBF 网络的混沌系统同步[J]. 物理学报,2001,50(9):1670-1674. (GUAN X P, FAN Z P, PENG H P, et al. The synchronization of chaotic systems based on RBF network in the presence of perturbation[J]. Acta Physica Sinica, 2001, 50(9):1670-1674.)

[8] 刘丁,任海鹏,孔志强. 基于径向基函数神经网络的未知模型混沌系统控制[J]. 物理学报,2003, 52(3):531-535. (LIU D, REN H P, KONG Z Q. Control of chaos solely based on RBF neural network without an analytical model[J]. Acta Physica Sinica, 2003, 52(3):531-535.)

[9] 何国光,曹志彤. 混沌神经网络的控制[J]. 物理学报, 2001, 50(11):2103-2107. (HE G G, CAO Z T. Controlling chaos in chaotic neural network[J]. Acta Physica Sinica, 2001, 50(11):2103-2107.)

[10] AYATI M, KHALOOZADEH H. Practical implementation of adaptive impulsive observer based chaotic synchronization scheme[J]//IEEE International Conference on System Science and Engineering(ICSSE), 2011, 44(10): 367-372.

[11] SHAN L, LIU Z, WANG Z. A new MLS chaotic system and its back stepping sliding mode synchronization control[J]. Journal of Computers, 2010, 5(3):456-463.

[12] CHERRIER E, M'SAAD M, FARZA M. High-gain observer synchronization for a class of time-delay chaotic systems: Application to secure communications[J]. Journal of Nonlinear Systems and Applications, 2010, 1(3/4):102-112.

[13] AYATI M, KHALOOZADEH H. Stable chaos synchronization scheme for non-linear uncertain systems[J]. IET Control Theory Applications, 2010, 4(3):437-447.

[14] BEHESHTI S, KHALOOZADEH H. Synchronization of time-delay chaotic systems in the presence of parameters uncertainties with sliding mode observer design[C]//The 2nd International Conference on Control, Instrumentation and Automation(ICCIA), 2011:664-669.

(上接第76页)

[3] GWALTNEY D A, BRISCOE J M. Comparison of communication architectures for spacecraft modular avionics systems[M]. Washington: NASA, 2006.

[4] MATSUBARA M, KOJIMA T, SHIMAMURA K, et al. Node status monitoring and state transition mechanism for network centric X-by-Wire systems[C]//Autonomous Decentralized Systems, USA: IEEE, 2009:1-6.

[5] BERGENHEM C, KARLSSON J. A process health status service for safety related systems using TT/ET communication scheduling[C]//Pacific Rim International Symposium on Dependable Computing, IEEE, 2008:122-131.

[6] MUDALLAR V S. Verfication of FlexRay membership protocol using UPPAAL[D]. Manhattan: Kansas State University, 2008.

[7] SAE S-18 Committee. ARP 4761 guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment[M]. USA: SAE, 1996.

[8] PFEIFER H. Formal verification of the TTP group membership algorithm[C]//Formal Methods for Distributed System Development FORTE XIII/PSTV XX, 2000:3-18.

[9] BAUER G, PAULITSCH M. An investigation of membership and clique avoidance in TTP/C[C]//Symposium on Reliable Distributed System, 2000:118-124.

[10] SAE International Group. TTP Communication protocol [Z]. 2011.

(上接第88页)

[8] 孙枫,吴旭,王根. 舰载机大失准角的快速二次传递对准方法[J]. 华中科技大学学报,2012,40(12):65-69, 74. (SUN F, WU X, WANG G. Rapid second time transfer alignment of large misalignment for carrier aircrafts[J]. Journal of Huazhong University of Science and Technology, 2012, 40(12):65-69,74.)

[9] 王司,邓正隆. 机载导弹空中二次快速传递对准方法研究[J]. 航空学报,2005,26(4):486-489. (WANG S, DENG Z L. Study on a twice rapid transfer alignment approach to missiles carried aboard in flight[J]. Acta Aeronautica et Astronautica Sinica, 2005, 26(4):486-489.)

[10] 秦永元,张洪钺,汪叔华. 卡尔曼滤波与组合导航原理[M]. 西安:西北工业大学出版社,2012. (QIN Y Y, ZHANG H Y, WANG S H. Theory of Kalman filter and integrated navigation[M]. Xi'an: Northwestern Polytechnical University Press, 2012.)