航天用时间触发网络系统同步性的故障分析*

赵 梦[1,2]，田文波[1,2]，罗 宇[1,2]，王冠雄[1,2]，刘 强[1,2]

（1. 上海航天电子技术研究所·上海·201109；
2. 中国航天科技集团有限公司第八研究院 智能计算技术重点实验室·上海·201109）

摘 要：确定性网络的同步性在航天电子系统中至关重要。为保证确定性网络在发生故障的情况下也能正常地进行时间同步，采用 spaceVPX 标准中典型的双星拓扑交换结构，配置基于时间触发以太网协议的可容错系统。针对此架构，对使用以太网的航天系统中发生故障的单容错结构进行了仿真，并模拟了几种时间同步协议控制帧异常的情况：协议控制帧包括冷启动帧、冷启动应答帧、集成帧，从故障交换机的端口发送到网络中的一个终端系统后，对于时间触发网络的同步网络所产生的影响。仿真结果表明，故障交换机会逐渐延长处于正常工作的终端系统的启动时间，不利于整个确定网络系统的同步过程，但是，如果设置不同协议控制帧的周期超过一定的数值后，单点故障不会影响双冗余系统的启动时间。

关键词：时间触发网络；冷启动异常分析；确定性网络的故障；航天电子系统

中图分类号：TN911.73；TP391.9 **文献标志码**：A **文章编号**：2096-5974(2022)02-0074-07

Fault Analysis of Synchronization of Aerospace Time-Triggered Network System

ZHAO Meng[1,2]，TIAN Wenbo[1,2]，LUO Yu[1,2]，WANG Guanxiong[1,2]，LIU Qiang[1,2]

（1. Shanghai Aerospace Electronic Technology Institute，Shanghai 201109；
2. The Eight Academy of China Aerospace Science and Technology Corporation，Key Lab of Intelligent Computing Technology，Shanghai 201109）

Abstract：The synchronization of deterministic networks is very important in aerospace electronic systems. In order to ensure the normal time synchronization of deterministic network in case of failure，this paper adopts the typical double star topology switching structure in spaceVPX standard to configure a fault-tolerant system based on time triggered Ethernet protocol. Aiming at this architecture，the single fault-tolerant structure in the aerospace system using Ethernet is simulated，and the exceptions of several time synchronization protocol control frames are simulated：the protocol control frame includes cold start frame，cold start response frame. The impact of the integrated frame sent from the port of the faulty switch to a terminal system in the network on the synchronization network of the time triggered network. The simulation results show that the fault switch will gradually prolong the start-up time of the terminal system in normal operation，which is not conducive to the whole synchronization process of the network system. However，if the period of different protocol control frames exceeds a certain value，the single point of fault will not affect the start-up time of the dual redundant system.

Keywords：time-triggered network；abnormal analysis of cold start；failure of deterministic networks；aerospace electronic system

---

* 收稿日期：2021-12-27；修回日期：2022-02-28

作者简介：赵梦（1995—），女，研究生。E-mail：623482389@qq.com

0　引　　言

在航空航天和汽车等安全性至关重要的行业中，需要在设备间使用高度可靠的通信。由于这些行业对于实时性、可靠性和容错性提出的更高要求，确定性网络如时间触发以太网（Time-Triggered Ethernet，TTEthernet）、精确时间协议（Precision Time Protocol，PTP）、FlexRay 总线、时间触发总线（Time-Triggered CAN，TTCAN）、SAFEbus、时间触发协议/ A 类（Time Triggered Protocol/class A，TTP/A）得到了广泛的应用[1]。尤其在航天电子设备朝着模块化、综合化和标准化的方向发展，星载信息量、综合化程度不断提升的过程中，网络中高质量的同步保证了可靠的确定性通信，因此提高接入以太网的设备之间正确的同步性是非常重要的。

TTEthernet 是从航空电子全双工交换式以太网（Avionics Full Duplex Switched Ethernet，AFDX）改进而来的，用于工业和航空电子应用的时间关键型网络[2-3]。它由 SAE AS6802 标准化，时间触发以太网运行在 OSI 第 2 层，与标准以太网完全兼容。通过使用混合基础设施支持时间触发（Time-Triggered，TT）、速率约束（Rate-Constrained，RC）和尽力而为（Best-Effort，BE）业务，从而满足严格的定时传输要求。其主要特点是基于全局同步的离线调度表的时间触发通信模式。在 TT 报文准备就绪且 RC 报文已经传输的情况下，采用抢占、及时阻塞和打乱次序三种集成方法解决冲突[1]。它还支持不同流量类别的虚拟分离，包括确定性和非确定性通信方式。时间触发以太网络的核心设备是集成不同流量类别数据流的交换机。而由关键应用程序生成的流量（以可预测的、确定性的方式传输）相对于非关键消息（以非确定性的方式传输）总是具有更高的优先级。确定性通信在延迟和可靠性方面有非常严格的要求，只有当观察到的链路没有被确定性通信流占用时，非确定性消息才会被传输[4-7]。

在航天领域，时间触发以太网络用于解决各有效载荷、航天器平台等相对独立的计算机之间，以及计算机内部各模块之间，高精度时基相对独立造成整体上的全局时钟偏差，进而导致共用信息不能精准到达的需求问题。时间触发以太网络架构设计在载人航天领域需要高安全关键等级的网络系统，因此设计要求使用冗余配置增强航天器内计算节点容忍故障的能力[8]。

在对可以兼容标准以太网的 SEA AS6802 同步协议分析之后，本文重点探究了时间触发以太网络中可能出现的几种异常情况及其对整个网络的启动时间产生的负面影响。一个或一系列协议控制帧（Protocol Control Frames，PCF），包括冷启动帧（Coldstart Frames，CS）、冷启动应答帧（Coldstart Acknowledge Frames，CA）、集成帧（Integration Frames，IN），从有故障的压缩主机（Compression Master，CM）传输到同步主机（Synchronization Master，SM），会增加 SM 正常的启动时间，在关键时刻发送 PCF 可以逐步增加启动时间[9]。

1　可容错 TTE 网络的硬件架构和仿真模型

本节描述了航天用可容错的时间同步网络的系统硬件架构和仿真模型的拓扑结构，航天领域工程应用中采用冗余备份的星型硬件架构如图 1 所示。这种双冗余式的硬件架构借鉴自 VITA78 SpaceVPX 标准中典型的双星拓扑交换结构，其中的冗余容错技术可以尽可能满足空间电子系统对于高可靠性应用的要求[9-10]。功能方面在普通以太网互连的基础上，还增加了时间同步和时间触发。此网络每个节点都有 2 个以太网接口，分别连接在 2 个交换节点上，互为备份关系。一部分节点连接在交换 1A/1B 上，另一部分节点连接在 2A/2B 上。压缩主机 CM 节点作为模块嵌入支持时间触发功能的交换机，和各个同步主机 SM 一起完成网络的同步。而仿真模型仿照硬件架构搭建，由于本次讨论需要探究故障 CM 对整个系统从上电到达一个稳定的同步状态所消耗的冷启动时间的影响，因此选取终端系统 sm4 和其中一个故障的压缩主机 CM-sw1 连接，如图 2 所示，此时 sm4 的状态变化会受到故障 CM-sw1 的直接影响[10-11]，如图 3 所示。

整个时间同步网络采用分布式的时钟部署方式，每个系统都有自己的时钟，而整个系统没有主时钟的概念[12]。基于时间触发以太网的同步服务系统能够以固定延迟和微秒级别的抖动同步通信。这些服务的核心是为了使分布式网络的终端系统和交换机中本地时钟同步起来，形成一个全局时钟[13]。

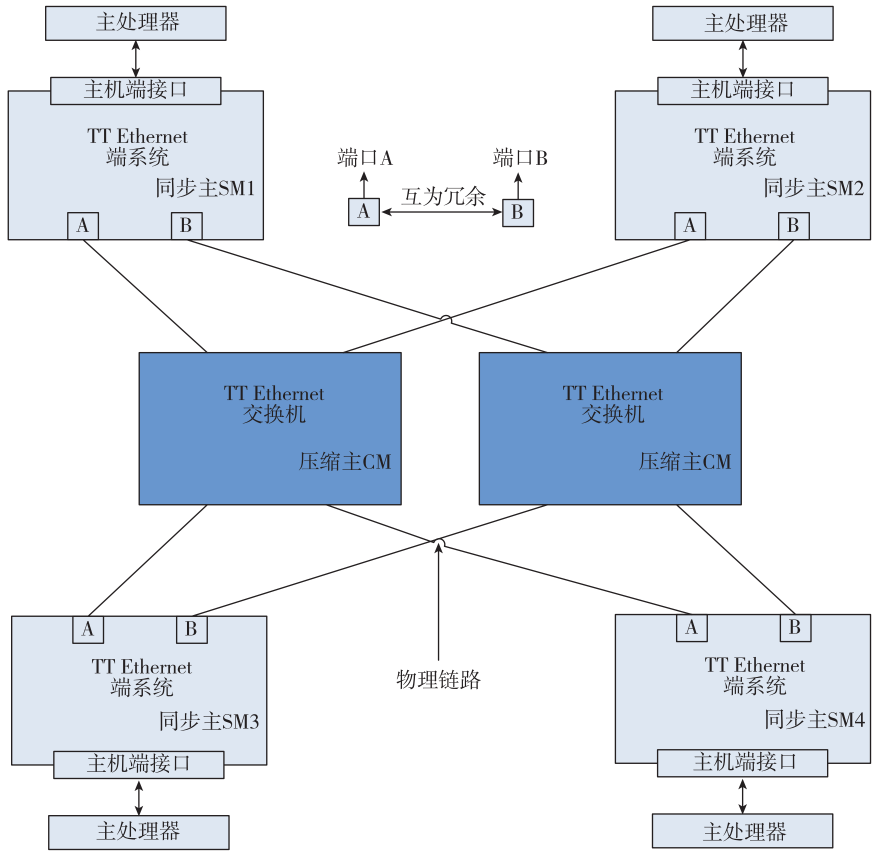

图 1　TTE 系统硬件架构

Fig. 1　TTE system hardware architecture

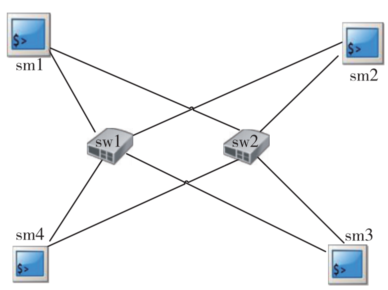

图 2　TTE 系统仿真模型

Fig. 2　TTE system simulation model

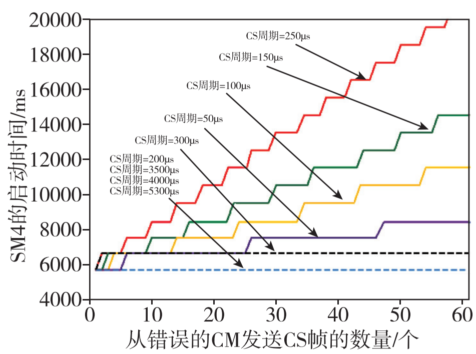

图 3　sm4 接收到出错的 CM 发送 CS 帧后的启动时间

Fig. 3　sm4's start-time after receives CS frame sent by faulty CM

2　故障情境下时间触发网络启动时间的仿真评估

2.1　故障模型概述

时间触发以太网的设计可以支持单故障和双故障假设。本文只关注单一故障对于设计的时间触发以太网络系统同步性的影响，在单故障假设下，时间触发以太网的目的是容忍终端系统的随机故障或交换机的不一致遗漏故障。时间触发以太网交换机可以配置具有执行保护中央总线的功能，该功能可实现即使一组终端系统发生任意故障，也可以将随机故障模式转换为不一致的遗漏故障模式[14-15]。特别考虑单一故障的原因是受空间辐射恶劣环境的影响，航天电子系统中存储电路等极易发生位翻转故障，因此采取冗余设计以及故障管理算法等进行故障诊断和隔离，从而达到吸收故障或者隔离故障的效果，使得某一模块或者系统的故障不会蔓延至其他模块或系统，由此单一故障发生的概率远大于多故障的概率[16]。

本节讨论在上述单故障模型下，网络异常可能对 TTEthernet 启动时间产生的负面影响。图 3 所示为 SM 的启动/重启过程状态机，其中 SM _ INTEGRATE，SM _ UNSYNC，SM _ FLOOD，SM _ WAIT _ 4 _ CYCLE _ START _ CS 是 4 个非同步状态，剩余的 3 个状态 SM _ TENTATIVE，SM _ SYNC，SM _ STABLE 为同步状态。网络的启动时间是指在观测到 SM 从上电启动到建立 SM _ STABLE 状态的时间。通过分析图 4 的 SM 的状态机可以看出，如果在一些时刻从 CM 接收到一些 PCF，则可以导致回退到较低的非同步状态或失去同步状态（从同步状态到非同步状态的转换）。例如，如果在同步状态之一中从 CM 接收到 CA 帧，则 SM 将过渡到 SM _ WAIT _ 4 _ CYCLE _ START _ CS 这个非同步状态。像这样的异常现象是本文分析的主要内容。

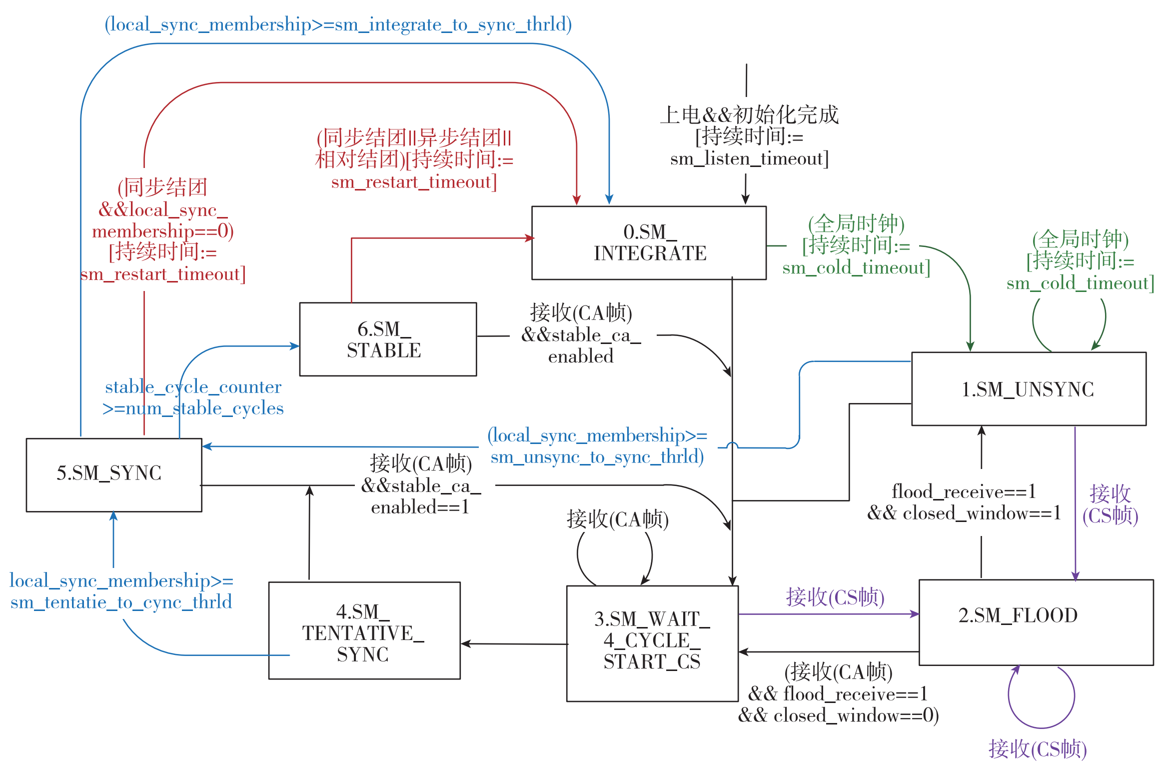

图 4　SM 的启动/重启过程状态机

Fig. 4　SM start/restart process state machine

2.2　仿真建立

根据 SAE AS6802 标准，采用 NS3 仿真系统完成对于网络中各个节点模块的开发，包括端系统、交换机，以及链路配置为双通道并模拟了硬件链路传输所具有的延迟。本文试验场景为其中一个压缩主机（CM）出现故障，其余设备（其他压缩主机 CM 和 4 个同步主机 SM）无故障。本文考虑的拓扑结构如图 3 所示。其中一个端口上的故障 CM 在 SM 的关键时刻传输 CS、CA 和 IN 帧序列。在此条件下，通过仿真估算了 SM 的启动时间。交换机 sw2 的故障端口连接到终端系统 sm4。

由于同步质量不受本研究的关注，而只考虑网络启动时间的影响，因此尽管模型支持非理想时钟，但网络组件中实现的本地时钟被设置为理想时钟。在所有仿真中，集成周期（Integration Cycles Duration，ICD）持续时间设置为 $T_{\mathrm{ICD}}=1000\mu\mathrm{s}$。

2.3　正常的启动

仿真结果表明，当观测到的网络中没有故障设备时，sm4 的默认启动时间为 $T_{\mathrm{d}}=5671\mu\mathrm{s}$。在这种情况下，冷启动过程反映了图 4SM 启动/重启过程状态机顺时针背景箭头所描绘的状态流转情况，在此过程中 SM 经历了以下状态转换：SM _ INTEGRATE → SM _ UNSYNC → SM _ FLOOD → SM _ WAIT _ 4 _ CYCLE _ START _ CS → SM _ TENTATIVE _ SYNC → SM _ SYNC → SM _ STA-

BLE。

2.4 故障的 CM 传输 CS 帧

1）SM 在 SM_WAIT_4_CYCLE_START_CS 状态下接收到 CS 帧：从图 4 的状态机中可以看出，sm4 在 SM_WAIT_4_CYCLE_START_CS 状态下接收到的 CS 帧，导致 sm4 转换到 SM_FLOOD 这个同步性较低的状态，sm4 在 SM_FLOOD 状态下会发送 CA 帧。由于无故障压缩主机 CM-sw2 处于不再接受 CA 帧的状态（此时网络的其余设备是正常地进行冷启动处理的），因此，sm4 将转换到 SM_UNSYNC 状态并开始发送 CS 帧。CM 的上述帧过滤机制将忽略这些 CS 帧。在接收到来自 CM-sw2 的 IN 帧之后，sm4 将转换到 SM_SYNC 状态，在足够的稳定周期之后，再转换到 SM 稳定状态。简而言之，发送给 SM 的 CS 帧在 SM_WAIT_4_CYCLE_START_CS 状态下会导致同步过程链发生变化：SM_INTEGRATE → SM_UNSYNC → SM_FLOOD → SM_WAIT_4_CYCLE_START_CS → SM_FLOOD → SM_UNSYNC → SM_SYNC → SM_STABLE，发生状态回退而后又进入同步状态。由分析可知，此异常将启动时间延长了相当一个集成周期的时间。

2）SM 在 SM_UNSYNC 状态下接收到 CS 帧：关注 SM_UNSYNC 状态附近的输入影响情况，可以看出，接收 CS 帧将导致 sm4 向 SM_FLOOD 状态的转换。在这种状态下，从故障 CM 接收到的 CS 帧可能会导致更早地过渡到 SM_FLOOD 状态。但是，由于 SM 不会在进入 SM_FLOOD 之后立即发送 CA 帧，因此提前过渡到 SM_FLOOD 状态不会加快 sm4 的启动速度。同时，无故障的 sw2 将转发来自另一个 SM 的 CS 帧，从而使 sm4 重新进入 SM_FLOOD 状态。其他 SM 在接收到上述 CS 帧后也将进入 SM_FLOOD 状态，这意味着所有 SM 都在同一时刻发送其 CA 帧。在这种情况下，sm4 的启动时间等于默认启动时间 T_d。

3）SM 在 SM_FLOOD 状态下接收到 CS 帧：在 SM_FLOOD 状态下接收到 CS 帧，将导致 SM 重新进入相同的状态。之后，当 SM 过渡到 SM_FLOOD 状态时，将发生与前面提到的 SM_WAIT_4_CYCLE_START_CS 状态相同的过程变化：SM_FLOOD → SM_WAIT_4_CYCLE_START_CS → SM_FLOOD → SM_UNSYNC → SM_SYNC → SM_STABLE。

总结 CS 帧序列的影响：如果从故障 CM 发送 CS 帧序列，根据序列中 CS 帧的数量及其周期，sm4 的启动时间将相应延长，因为每个接收到的 CS 帧都重新进入 SM_FLOOD 状态，该场景的模拟如图 3 所示，其中从 sw1 发送的 CS 帧的序列长度增加，同时改变这些帧之间的周期。序列的第一个 CS 帧在接近 SM_FLOOD 状态结束时到达 sm4。从结果可以看出，CS 帧的周期为 200μs 或大于 3500μs，对 sm4 的启动没有影响；而对于 300μs 的周期，只有第一个 CS 帧延长了一个集成周期（T_{ICD}）值的启动时间；对于其他时段，启动时间函数呈阶梯形，并随 CS 帧数的增加而增加，增量不是连续的，而是集成周期（T_{ICD}）值的倍数。这些值可以当作是 sm4 在重新进入 SM_FLOOD 状态时被阻塞的时间。启动时间函数呈阶梯形的原因在于一系列状态转换。

在从 CM-sw1 发送的 CS 序列结束之后，sm4 将从 SM_FLOOD 转换到 SM_UNSYNC 状态。然后，sm4 从已经同步的非故障 CM-sw2 接收帧内信号，并进入 SM_SYNC 状态，接着进入 SM_STABLE 状态。sm4 在 SM_UNSYNC 状态下花费的时间并不重要：在从 sw2 接收到 IN 帧之后，sm4 立即转换到 SM_SYNC 状态。而当 CS 帧的周期大于 3500μs 时，单个故障的 CM 不会影响网络的启动和建立时间同步的时长。

2.5 故障的 CM 传输 CA 帧

有故障的 CM 传输 CA 帧时的情形与故障的 CM 传输 CS 帧的情形非常相似。对于这种情况，当 sm4 接近 SM_WAIT_4_CYCLE_START_CS 状态的末尾时，故障 CM 开始传输 CA 帧，得到图 5 所示的梯形折线图。考虑到 CA 帧对 SM 的所有状态都有影响，这些帧之间的任何一个周期都会对基于时间触发网络的同步过程产生决定性的影响。每个接收到的 CA 帧都将导致转换到 SM_WAIT_4_CYCLE_START_CS 状态。一个特例是：在SM_STABLE 状态下，接收到 CA 帧且参数 stable_ca_enabled 配置正确，才可以转换到 SM_WAIT_4_CYCLE_START_CS 状态。在这种情况下，CA 帧之间的周期应该足够长，以便 SM 在下一个从 CM 传输的 CA 帧到达之前建立 SM_STABLE 状态。如图 5 所示，CA 帧的一个周期要大于 4500μs，此时单个故障的 CM 对于 sm4 等网络中

运行正常设备的启动以及时间同步没有影响。

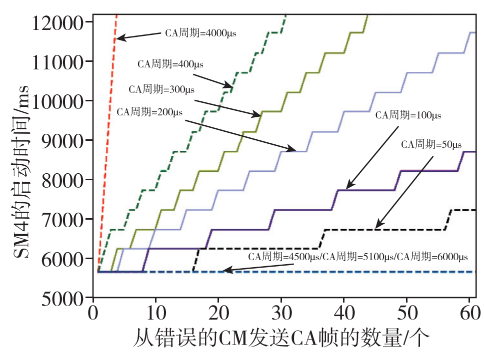

图 5　sm4 接收到故障的 CM 发送 CA 帧后的启动时间

Fig. 5　sm4's start-time after receives CA frame sent by faulty CM

2.6　故障的 CM 传输 IN 帧

来自故障 CM 的错误的 IN 帧会触发正常运转 CM 的异步/相对团功能，从而导致系统失去同步状态。图 6 显示了当 IN 帧处于 SM _ TENTATIVE _ SYNC 状态时，超出计划到达 sm4 情况的有关结果。如果帧间的周期比较短，则函数呈阶梯形，如果帧间的周期比较长，则函数呈线性。当在 SM _ TENTATIVE _ SYNC 状态下检测到异步/相对团时，SM 应过渡到 SM 非同步状态，在该状态下，开始传输 CS 帧。由于非故障 sw2 已经处于同步状态，它将忽略接收到的 CS 帧，同时将向 sm4 发送一个压缩的 IN 帧。然后，sm4 将再次转换到 SM 同步状态。综上，如果在 SM _ TENTATIVE _SYNC 状态下接收到除了 IN 帧外的其他序列，则将发生以下过程变化：SM _ TENTATIVE _ SYNC → n ×（SM UNSYNC → SM _ SYNC）→ SM _ STABLE。在 SM _ STABLE 状态下接收到计划外的帧序列也将会使得系统失去同步态。如图 6 所示，如果 IN 帧周期大于 4000μs，故障的 CM 发送错误的 IN 帧对于网络内正常运行的设备的启动和时间同步的建立与正常启动所需时长相同。通常，IN 帧长时间间隔对启动时间影响不大，但存在在 SM _ STABLE 状态下失去同步状态的风险 。

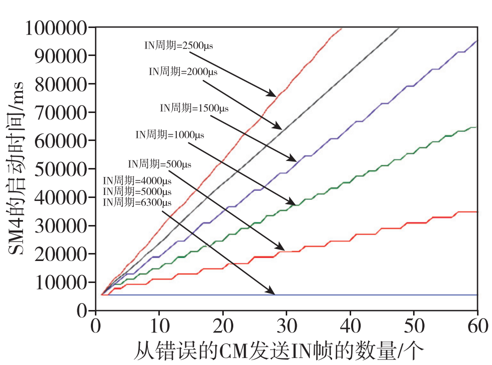

图 6　sm4 接收到故障的 CM 发送 IN 帧后的启动时间

Fig. 6　sm4's start-time after receives IN frame sent by faulty CM

由以上讨论可知，由于双压缩主机的备份容错机制，即使其中一个 CM 出现故障，另一个 CM 也会完成正常操作，发出正确的帧，同步主机（SM）通过接受窗口（acceptance _ window）的开闭规则过滤掉来自故障 CM 的部分错误协议控制帧（PCF），从而保证系统的启动可以正常运转，但是这个恢复过程在某些情景下会以延长启动时间为代价[2]。经仿真结果可知，在此时间触发网络仿真模型下，如有一个压缩主机（CM）发生故障，设置 CS 帧周期大于 3500μs，CA 帧周期大于 4500μs 且 IN 帧周期大于 4000μs 时，时间触发网络完成启动的时间和无故障情况下的正常启动时间相同。

3　结　　论

在容错系统中，具有处理意外情况的机制是非常重要的。以太网的单一容错配置可以处理一个故障组件：交换机或终端系统。文中模拟了一个端口上的故障交换机开始不受控制地传输单个和序列 PCF 的情况。结果表明，故障 CM 发送错误的 CS、CA 和 IN 帧，对时间触发网络的启动时间有影响，PCF 对确定性时间触发网络的同步性影响在到达临界时刻表现得尤为明显。但是如设置协议控制帧的周期超过一定数值后，单点故障双冗余系统的启动时间和正常启动的时间相同，为航天领域等使用双冗余时间触发以太网的系统中参数设置提供参考。下一步将重点研究分析故障端系统脱离控制后，随机地将 PCF 序列发送到同步的时间触发网络产生的影响。

参考文献（References）

[1] 何向栋，孙靖国，陈长胜，等. SAE AS6802 协议研究及模块化仿真平台设计［J］. 计算机工程，2021，47（1）：203-209.
HE X D，SUN J G，CHEN C S，et al. SAE AS6802 protocol

research and modular simulation platform design [J]. Computer Engineering，2021，47（1）：203-209（in Chinese）.

[2] SAE Technical Standard. SAE AS6802 [S]. SAE International，2011.

[3] 张巍，蒋乐天，罗泽雄．基于时间触发架构的网络技术研究与设计[J]．航空电子技术，2017，48（2）：44-49.
ZHANG W，JIANG L T，LUO Z X. Network technology research and design based on time-triggered architecture [J]. Avionics Technology，2017，48（2）：44-49（in Chinese）.

[4] AMIN S，OBERMAISSER R. Time-triggered scheduling of query executions for active diagnosis in distributed real-time systems [C] //Proceedings of 2017 22nd IEEE International Conference on Emerging Technologies and Factory Automation（ETFA）. Limassol，Cyprus：IEEE，2017：1-9.

[5] 徐乾舜，华更新．基于空间应用的TTE时钟同步算法研究[J]．计算机测量与控制，2018，26（7）：271-275，281.
XU Q S，HUA G X. Research on TTE clock synchronization algorithm based on space application [J]. Computer Measurement and Control，2018，26（7）：271-275，281（in Chinese）.

[6] 钟程，张磊，凌震．基于时钟精度加权的时钟同步算法[J]．航天控制，2020，38（2）：69-73.
ZHONG C，ZHANG L，LING Z. Clock synchronization algorithm based on clock precision weighting [J]. Aerospace Control，2020，38（2）：69-73（in Chinese）.

[7] STEINER W，DUTERTRE B. Layered diagnosis and clock-rate correction for the TTEthernet clock synchronization protocol [C] // Proceedings of IEEE Pacific Rim International Symposium on Dependable Computing. Niigata，Japan：IEEE，2012.

[8] 汤雪乾，李峭，孔韵雯，等．时间触发以太网拜占庭容错方法的形式化验证[J]．载人航天，2018，24（2）：273-278.
TANG X Q，LI Q，KONG Y W，et al. Formal verification of Byzantine fault-tolerant method in time-triggered Ethernet [J]. Manned Spaceflight，2018，24（2）：273-278（in Chinese）.

[9] 康旭辉，连剑，赵雪纲．基于SpaceVPX架构的星上高速载荷数据实时处理平台设计[J]．航天器工程，2018，27（4）：98-103.
KANG X H，LIAN J，ZHAO X G. Spaceborne high-speed hayload data real-time processing platform design based on SpaceVPX architecture [J]. Spacecraft Engineering，2018，27（4）：98-103（in Chinese）.

[10] MURSHED A，OBERMAISSER R. Scheduler for reliable distributed systems with time-triggered networks [C] // Proceedings of 2017 IEEE 15th International Conference on Industrial Informatics（INDIN）. Emden：IEEE，2017：425-430.

[11] 杨俊雄，徐亚军，何锋，等．时钟同步精度对TTE实时性影响研究[J]．电光与控制，2016，23（8）：33-38.
YANG J X，XU Y J，HE F，et al. Research on influence of clock synchronization accuracy to TTE real-time performance [J]. Electronics Optics & Control，2016，23（8）：33-38（in Chinese）.

[12] 刘晚春，李峭，何锋，等．时间触发以太网同步及调度机制的研究[J]．航空计算技术，2011，41（4）：122-127.
LIU W C，LI Q，HE F，et al. Research on time-triggerd-Ethernet synchronization and scheduling mechanism [J]. Aeronautical Computing Technique，2011，41（4）：122-127（in Chinese）.

[13] 张金国．TTE交换机FPGA设计及实现[D]．成都：电子科技大学，2020.
ZHANG J G. FPGA design and implementation of TTE switch [D]. Chengdu：University of Electronic Science and Technology of China，2020（in Chinese）.

[14] ZHANG Y，FENG H，LU G，et al. Clock synchronization compensation of Time-Triggered Ethernet based on least squares algorithm [C] //Proceedings of IEEE/CIC International Conference on Communications in China. Chengdu：IEEE，2016.

[15] DUTERTRE B，EASWARAN A，HALL B，et al. Model-based analysis of timed-triggered ethernet [C] // Proceedings of IEEE/AIAA Digital Avionics Systems Conference. Los Angeles：IEEE，2012.

[16] GAETANO C，LUCA D C，SAVERIO M. Controlling queuing delays for real-time communication [J]. ACM SIG-COMM Computer Communication Review，2018，46（3）：1-7.