パーティショニング RTOS 向けユーザーモード TCP/IP プロトコルスタックにおける時間パーティショニングに関する研究

M2021SE005 板田怜子
指導教員：本田晋也

1　はじめに

航空機や宇宙機などの信頼性が要求される組込みシステムでは，システムを安全度水準が異なる複数のアプリケーションに分割して，それらの空間的・時間的な独立性を保証して実行したいという要求がある．そのため，空間的・時間的な独立性を実現するパーティショニング機構を持つ RTOS であるパーティショニング RTOS（以下，P-RTOS）を利用することが求められている．P-RTOS により実現される実行環境をパーティショニング実行環境と呼ぶ．空間的なパーティショニングは一般の RTOS でも実現されているメモリ保護やアクセス保護で実現することが可能である．一方，時間的なパーティショニングは多くの RTOS では実現されていない．

航空機向けの RTOS 仕様では [1]，システムに一定の周期（システム周期）を設定して，その周期をタイムウィンドウと呼ばれる時間に分割して固定的に各アプリケーションを割り当てる TDMA スケジューリングと呼ばれる方法が採用されている．TDMA スケジューリングを用い，アプリケーション毎にタイムウィンドウを割り当てて実行することで，アプリケーション間の時間パーティショニングを実現することが可能である．

しかしながら，ミドルウェアのパーティショニング実行環境での実現方法は検討されていない．本研究におけるミドルウェアとは，通信プロトコルスタックのように，他のアプリケーションとは独立してコンテキストを持ち動作するソフトウェアであり，複数のアプリケーションからの要求や外部からの要求に応じて処理を行う．既存のミドルウェアはカーネルモードで動作することを前提に開発されている．しかしながら，システムによっては，ミドルウェアに要求される安全度水準が低い場合があり，ユーザーモードかつタイムウィンドウ内で動作するように構成を変更する必要がある．

本研究は，先行研究を引き継ぎ，TCP/IP プロトコルスタックを対象にパーティショニング実行環境での実現を目的とする．具体的には，基本性能評価としてパーティショニング RTOS を使用しない場合や TDMA スケジューリングを有効とした場合との性能評価の実施及び，TDMA スケジューリングへ影響及ぼす処理の分析と評価及び改善を実施する．

2　先行研究

先行研究 [2] では，TCP/IP プロトコルスタックを時間パーティショニング機構を持つ RTOS のユーザーモードで実現する初期検討として，TINET と呼ばれる TCP/IP プロトコルスタックを対象に図 1 に示すランタイム構成を提案している．提案手法では，TCP/IP プロトコルスタックに専用のパーティションを用意して実行する．各アプリケーションは，サービスコールとして実現された TCP/IP 送受信受付用 API を呼び出して送受信を行う．アプリケーション毎にプロキシタスクを用意してサービスコール経由の要求を受け取り，TCP/IP プロトコルスタック本体の TCP/IP 送受信受付用 API を呼び出す．

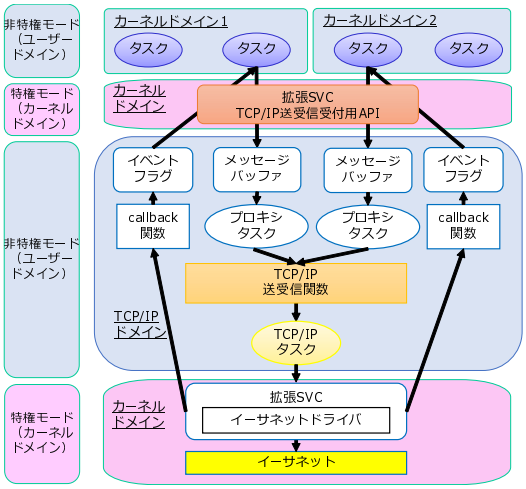

図 1　ユーザーモード TCP/IP プロトコルスタック

3　研究課題

先行研究 [2] を踏襲し，TCP/IP プロトコルスタックのユーザーモードでの実現手法の提案と評価を実施する．先行研究では，次の課題がある．

- P-RTOS を使用しない場合や TDMA スケジューリングを有効とした場合との性能評価が未実施である．
- イーサネットドライバはカーネルモードで動作するため，他のユーザードメインの実行を阻害する可能性がある．その影響度の評価を行い，ユーザーモード化と性能への影響を評価する．

4　背景技術

4.1　安全度水準

安全度水準とはシステムに要求される安全の度合いを表す．不具合が発生した場合の影響が大きい機能ほど安全度水準が高く設定される．安全度水準が高いほど，開発に必要なコストが大きい．安全度水準は，ASIL（自動車安全水準）や SIL（機能安全度水準）等があり，安全規格により定められている．

システムによっては複数の機能（サブシステム）で構成されており，サブシステムごとに要求される安全度水準が異なる場合がある．パーティショニング機構がない

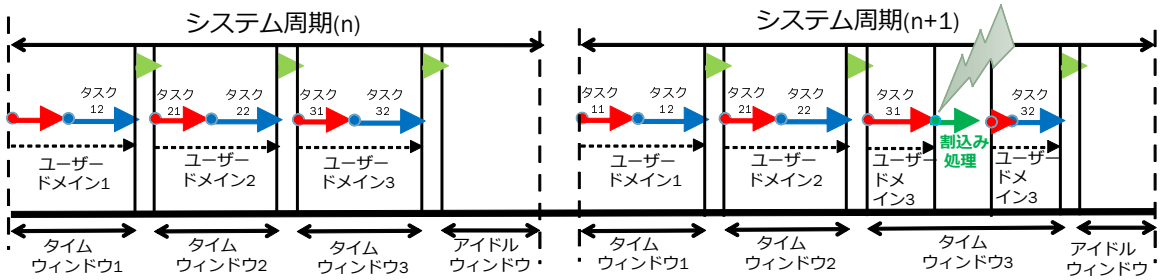

図 2　TDMA スケジューリングによる時間パーティショニング

環境で実現すると次の 2 つの問題が発生する．

- 全サブシステムを安全度水準が最も高いサブシステムの安全度水準とする必要がある．
- あるサブシステムを変更すると全てのサブシステムの再検証が必要となる．

4.2　FFI の実現

前述の問題を解決するためには，Freedom from interference（FFI）を実現すればよい．FFI とはサブシステム間の空間・時間的な干渉がないことである．そして FFI はパーティショニング機構により実現可能である．具体的には，サブシステムの実行に制限をかけられるユーザーモードで実行することで，パーティショニングを実現する．

4.3　パーティショニング環境

パーティショニング機構には空間パーティショニングと時間パーティショニングがある．

空間パーティショニングとは，サブシステムを許可されたメモリにのみアクセス可能とすることである．

時間パーティショニングとは，あるサブシステムの時間的な振る舞いの変化が，他のサブシステムに影響を及ばさないようにすることである．これは，図 2 に示す TDMA スケジューリングにより実現される．まず時間枠にシステム周期を定め，システム周期をいくつかのタイムウィンドウに分割する．次にタイムウィンドウに，いずれかのサブシステムが割り当てられ実行される．そしてサブシステムに属するタスクは，割り当てられたタイムウィンドウ内でスケジューリングされ実行される．

5　研究対象のシステム

本研究では，JAXA の次世代宇宙機向け CPU を対象とし，TCP/IP プロトコルスタックのパーティショニング環境での実行方法を実現する．

JAXA の次世代宇宙機向け CPU は Ethernet 機能を持つ [5] が，TCP/IP 通信の安全度水準は低く，重要な通信は安全度水準が高い SpaceWire ネットワークを使用する．

P-RTOS については，TOPPERS/HRMP3 カーネルと呼ばれるマルチコア向けの P-RTOS が用意されている．JAXA の CPU は設計中であるため，互換性が高い既存のシングルコアのチップを使用する．また本研究の P-RTOS はシングルコア対応の TOPPERS/HRP3 カーネル（以下，HRP3 カーネル）を用いる．TCP/IP プロトコルスタックは ITRON TCP/IP 仕様の TINET を使用する．

5.1　HRP3 カーネル

HRP3 カーネルとは，ITRON 仕様をベースとして，空間パーティショニングと時間パーティショニング機構を追加した RTOS である．またサブシステムに相当する概念として保護ドメインを定義する．保護ドメインはユーザードメイン，カーネルドメインから成り立つ．ユーザードメインとは，複数定義可能であり，ユーザーモードで実行される．ユーザードメインのリソースはお互いアクセス出来ない．カーネルドメインとは，1 つのみ存在し，カーネルモードで実行され，全てのリソースへのアクセスが許可されている．

5.2　空間パーティショニング

空間パーティショニングでは，あるユーザードメインが他の保護ドメインや RTOS のメモリへアクセスできないように設定する．この制限は，Memory Protection Unit（MPU）と呼ばれるハードウェアによって実現される．MPU の領域情報を，実行中の保護ドメインに許可されたメモリ領域へのアクセスを許可し，それ以外の実行中でない保護ドメインのメモリ領域へのアクセスを禁止するよう設定することでメモリ保護を行う．他の保護ドメインにディスパッチするときは，MPU に設定している領域情報を P-RTOS が切り換える．

5.3　時間パーティショニング

時間パーティショニングは，TDMA スケジューリングより各ユーザードメインを実行する．ユーザードメインを繰り返し実行する基本的な周期をシステム周期と呼ぶ．またユーザードメインをどう繰り返し実行するか，システム動作モード毎に設定することができる．システム周期内の連続した時間区間をタイムウィンドウと呼ぶ．

1 つのユーザードメインに複数のタイムウィンドウを割り当て，タイムウィンドウ内は割り当てたユーザードメインに属するタスクを実行する．タスクは，システム周期毎にタイムウィンドウに登録された順に実行する．

カーネルドメインにはタイムウィンドウを割り当てることはできない．カーネルドメインに属するタスクは，実行状態になると実行中のタイムウィンドウに属するユーザードメインのタスクより優先度が高いとタイムウィンドウを無視して実行される．

表 1 基本性能評価の構成

構成	OS	アプリケーション	TCP/IP プロトコルスタック	スケジューリング
ASP	パーティショニングレス RTOS	無効（カーネルモード）	カーネルモード	優先度ベース
AU-TK	P-RTOS	ユーザーモード	カーネルモード	優先度ベース
AU-TU	P-RTOS	ユーザーモード	ユーザーモード	優先度ベース
AU-TU-T	P-RTOS	ユーザーモード	ユーザーモード	TDMA スケジューリング

6 基本性能評価

研究課題で述べた先行研究で未実施の基本的な性能評価を実施する．

6.1 評価環境

評価ハードウェアは，RX64M 120Mhz を搭載した北斗電子社製の HSBRX64MC を用いた．イーサネットコントローラは，RX64M 内蔵の ETHERC（100MbE）を使用した．評価は，PC と評価ボードのみをハブに接続して行った．

評価ハードウェア上でエコーサーバータスクを実行し，PC から 10byte 送信してエコーサーバーからデータが返ってくるまでの時間を 1000 回計測する．

6.2 評価対象の構成

基本性能評価の構成を表 1 に示す．

構成 ASP は，HRP3 カーネルのパーティショニング機能なし版の ASP カーネルを使用し，全てプログラムはカーネルモードで実行し優先度ベースでスケジューリングされる．その他の構成では，HRP3 カーネルを用いた．

構成 AU-TK は，使用している OS 以外は構成 ASP と同じ条件である．時間パーティショニングは無効で優先度ベースでスケジューリングされる．また，アプリケーションをユーザーモードで実行している．

構成 AU-TU は，構成 AU-TK から TCP/IP プロトコルスタックをユーザーモードで実行するよう変更している．

構成 AU-TU-T は，構成 AU-TU から，TDMA スケジューリングを用いて時間パーティショニングを有効としている．システム周期を 1500us に設定しタイムウィンドウを 400us に設定したものを 3 つ用意し，1 個のタイムウィンドウでアプリケーション（エコーサーバータスク）を，もう一つのタイムウィンドウで TCP/IP プロトコルスタックを動作させる．

6.3 評価結果

図 3 に評価結果を示す．構成 ASP/AU-TK は実行時間はおおよそ 200us になり，OS やユーザーモード化による性能の低下は見受けられなかった．しかしながら，HRP3 カーネルを用いた構成 AU-TK は，応答時間が他の数倍となるケースが観測された．

構成 AU-TU は，実行時間はおおよそ 400us になり前述の 3 つより 2 倍ほど遅くなった．これは，TCP/IP プロトコルスタックがユーザーモードとなったことにより，プロキシタスク経由で TCP/IP の API を呼び出すためであると考えられる．

構成 AU-TU-T は，他の環境と比較して実行時間は 1500〜3000us の間で変動している．これは，TDMA スケジューリングのシステム周期が 1500us であるため，エコーサーバーがデータ受け取って返すまでに最長の場合約 2 システム周期（3000us）必要であるためと考えられる．

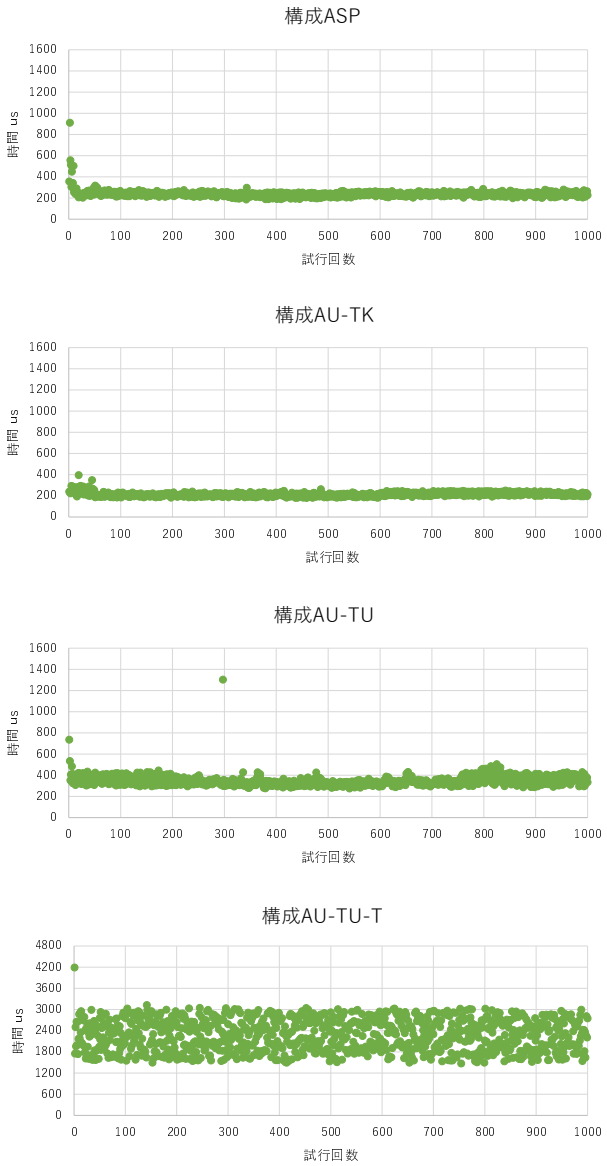

図 3 基本性能評価の計測結果

7 カーネルモードの処理

7.1 処理の概要

TDMA スケジューリングへ影響を及ぼすものとしてカーネルモードで動作する処理がある．ユーザーモード化した TINET では次の 4 つの処理が該当する．これら

表 2 構成 AU-TU: カーネルモード処理の最悪値

カーネルモードの処理概要	最悪値
TCP/IP の API 呼び出し	7.7us
イーサネットドライバ	92.66us
イーサネットドライバの割込みハンドラ	2.3us
Memcopy	3.0us

の処理がカーネルモードで動作している理由は以下の通りである．

- TCP/IP の API 呼び出し
  TCP/IP の API 呼び出しは，拡張サービスコールとしてカーネルモードで動作する．アプリケーションが指定したメモリ領域がそのアプリケーションからアクセスできるかチェックするため，カーネルモードで実行する必要がある．
- イーサネットドライバの割込みハンドラ
  HRP3 カーネルでは，割込みハンドラは必ずカーネルモードで実行する必要がある．
- イーサネットドライバ
  イーサネットドライバの割込みハンドラがカーネルモードであるので，イーサネットコントローラもカーネルモードで実現されている．
- Memcopy
  ユーザーモードで動作する TCP/IP プロトコルスタックでは，別のドメインのアプリケーションに API で指定されたメモリ領域に対する読み書きができないため，カーネルモードで動作させる．

7.2 計測結果

TDMA スケジューリングへ影響を及ぼすカーネルモードで動作する処理時間を計測するため，構成 AU-TU において送受信するデータを 100byte としエコー処理計測を 10 回実施し，各処理の実行時間をロジック・アナライザを用いて計測した．各処理の最悪値を表 2 に示す．TDMA スケジューリングにおけるタイムウィンドウの幅はシステムにもよるが，1000us 単位で設定することが多いと考えている．計測結果より，イーサネットドライバ以外は数 us と十分小さい値であり，対策の必要はないと判断した．

7.3 イーサネットドライバーのユーザーモード化

TDMA スケジューリングへの影響が最も大きいイーサネットドライバのユーザーモード化を検討する．イーサネットドライバは，その割込みハンドラとはデータ共有はしておらず，OS の API で通信しているため，ユーザーモード化が可能であることが分かった．そこで，イーサネットコントローラを TCP/IP ドメインからアクセス可能とすることで，イーサネットドライバをユーザーモードとして動作するよう変更した．

ユーザーモード化したイーサネットドライバを用いた構成 AU-TU，AU-TU-T のエコー処理の性能を評価した．測定結果を図 4 に示す．図 3 の結果と比較すると，両方の構成において，実行時間の増加は発生していない．

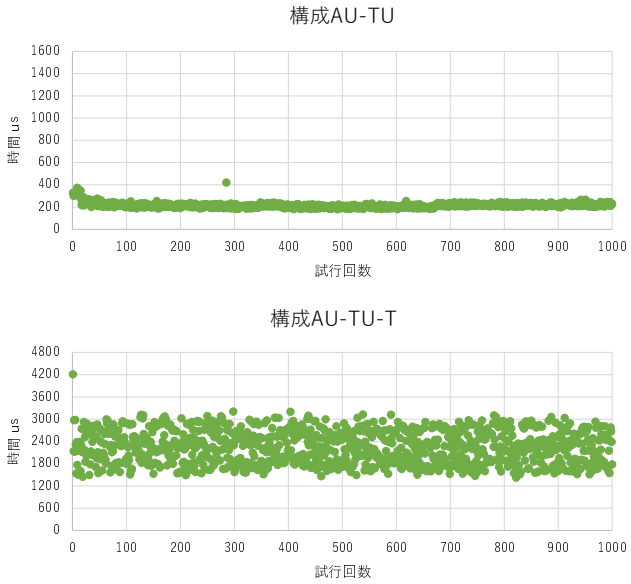

図 4 ユーザーモードドライバを用いた計測結果

8 おわりに

本研究では，ユーザーモード TCP/IP プロトコルスタックの各種構成での実行時間の変化について明らかにした．次に，TDMA スケジューリングへ影響を及ぼすカーネルモード処理が，時間パーティショニングに影響を与えるかを評価し，イーサネットドライバをユーザーモード化した．今後の課題としては，複数のアプリケーションが TCP/IP プロトコルスタックを共有する状況において，各アプリケーションからの送信帯域を保証する手法の提案と実現及び評価の実施が挙げられる．

参考文献

[1] Airlines Electronic Engineering Committee (AEEC), Avionics Application Software Standard Interface (ARINC Specification 653-1), ARINC Inc., 2003

[2] 手塚湧太郎, 本田晋也, 大谷寿賀子, 枝廣正人, ”パーティショニング OS 向けユーザモード TCP/IP プロトコルスタック”, 情報処理学会研究報告, Vol.2022-EMB-59,No.33, pp. 1-8, オンライン, Mar. 2022.

[3] 伊藤弘将，松原豊，高田広章，ミドルウェアに対する Coverage-based Greybox Fuzzing の適用, 情報処理学会論文誌, Vol.62,No.3, pp. 877-890, Mar 2021.

[4] D. Reinhardt, M. Guntner, and S. Obermeir. ¨Virtualized Communication Controllers in Safety-Related Automotive Embedded Systems. In Architecture of Computing Systems (ARCS), 2015 28th International Conference on, Mar. 2015.

[5] 三菱重工株式会社. 三菱重工技報 vol.58 no.4 (2021) 航空宇宙特集.