平成28年度 情報工学コース卒業研究報告要旨

高田・本田 研究室	氏　　名	石 野　正 敏
卒業研究題目	ミックスドクリティカルシステム向けイーサネットコントローラ共有機構	

近年，自動車は多機能化が進み，求められる信頼度の異なるシステムが混在している．このようにシステム内に求められる信頼度が異なるシステムが混在しているものをミックスドクリティカルシステムという．昨今の自動車には多くの機能を実現するために多くのECU が搭載されているが，機能ごとにひとつの ECU を使用していると数が膨大になり限られた自動車の空間内では容量が不足してしまう．そのため，将来的にマルチコアプロセッサを利用して，複数の機能をひとつの ECU に実現できるようになると，求められる信頼性の異なる機能がプロセッサ内に混在することになり，ミックスドクリティカルシステムになってしまう．

しかし，車載制御システムには高い信頼性が求められ，ISO26262 に基づく安全規格に従う設計が必要である．安全規格に従うために，求められる信頼度が異なるシステムを信頼度ごとにパーティショニングするような手法がとられている．プロセッサ内であれば保護機能付きの RTOS を利用することで，高信頼パーティショニングと低信頼パーティションが使用するメモリ領域を制限することでができる．しかしながら，それぞれのパーティションが単純にネットワークデバイスを共有すると，高信頼パーティションの信頼性が低信頼パーティションによって脅かされる危険性が存在する．そのために，高信頼パーティションのみがデバイスを専有し，低信頼パーティションがデバイスを使用したい場合は処理を高信頼のパーティションに依頼するような方式があり，これを依頼方式と呼ぶ．しかし，この方式を用いると，高信頼のパーティションが低信頼パーティションからの依頼を受け取る処理や，低信頼パーティションと高信頼パーティション間でのデータの受け渡し処理などが発生するためオーバーヘッドが増加してしまうという問題がある．その他にも高信頼パーティションが低信頼パーティションからの連続的な送信依頼により Dos 攻撃を受けるという問題がある．

従来では車載システムにおけるネットワーク通信では CAN が使われており，求められる信頼性の異なるパーティションで CAN コントローラを安全に共有する手法として ProtectionWrapper を用いた方法が提案されている．ProtectionWrapper は保護対象のデバイスに対してアクセス制御を行う機構で，低信頼パーティションが不正にデバイスの制御レジスタを書き換えることを防ぐことができる．しかし，最近ではデータサイズの大きいデータを ECU 間でやり取りする必要が出てきており，帯域幅の大きいイーサネットを車載システムにおけるネットワーク規格として用いる試みがなされるようになってきている．

本論文では，まず依頼方式によってイーサネットコントローラを共有する機構を実現した．そして，依頼方式とは別な手法として，低信頼パーティションが送受信の処理を行う際に高信頼パーティションに処理を依頼せずに低信頼パーティション自身が処理を行いながらも，高信頼パーティションの時間的及び空間的保護を実現するために必要な機能を検討し，一部実装した．