TCP/IP vulnerabilities in embedded devices for accelerator control

Takashi Sugimoto[1,A)], Miho Ishii[A)], Takemasa Masuda[A)]
Toru Ohata[A)], Tatsuaki Sakamoto[A)], Ryotaro Tanaka[A)]

[A)] Japan Synchrotron Radiation Research Institute (JASRI/SPring-8)
1-1-1 Kouto, Sayo, Hyogo, 679-5198

Abstract

Recent accelerator-control system consists of many embedded devices, which are equipped with Ethernet interface. By increasing the number of Ethernet-connected devices and TCP/IP implementation, more trouble have arisen. Present study aims at revealing network vulnerabilities in the embedded devices to improve operation stability at SPring-8. One of the embedded devices, motor control unit (MCU), was investigated, and we succeeded in finding vulnerability corresponding to load of network traffic. Strategies for improving reliability of the MCU and embedded devices are presented.

加速器制御用組み込み機器におけるTCP/IP脆弱性

１．研究の背景

1-1. 制御機器と通信インターフェース

加速器の高度化に伴い、より多数の計測・制御機器が使用されるようになってきている。従来、機器の制御には主にRS-232CやGPIBインターフェースが用いられてきた。これらの従来の通信インターフェースは1対1あるいは1対少数の短距離・小容量通信に留まっている。

近年、計測機器・制御機器のイーサネットインターフェースの標準化が進んできている。イーサネットは計算機の標準通信インターフェースとして普及しており、RS-232CやGPIBのような従来のインターフェースと比較して、1) 多対多の接続トポロジー, 2) 長距離通信, 3) 広帯域, 4) 比較的安価 といった長所がある。加速器のような大規模制御システムをRS-232CやGPIBだけで制御することはもはや困難であり、今日ではイーサネットと標準プロトコルTCP/IPが積極的に利用されている。

計測・制御機器の多くは汎用計算機とは異なり、特定の目的のために必要最低限のハードウェアで構成される「組み込み機器」である。組み込み機器はハードウェア性能の制限のため、多くの場合、ハードウェア専用OSや汎用計算機用OSのサブセット版を使用している。ベンダや実装が異なる機器がネットワークに接続された場合、互換性の欠如や性能の不足に起因する障害が発生することがある。

1-2. SPring-8における組み込み機器

SPring-8ではMADOCAフレームワークに基づいたTCP/IPベースの制御システムが構築されている。図1は制御系ネットワークへのIPアドレス登録機器数の変遷を示す。ネットワークトポロジーが更新[1]された2001年以後機器数は年々増えており、2001年1月の342台から2008年3月の1141台まで、加速器制御ネットワークへの接続機器数は3倍以上に増加した。増加数の多くは、VME仮想ホストの増加と、組み込み機器インターフェースのGPIBからイーサネットへの変更に伴う制御系ネットワークへの新規接続である。機器数の増加に伴い、ネットワーク通信異常に起因する加速器の運転への影響が顕著となってきている; 例えば、デジタルマルチメーターの通信障害、オシロスコープの通信障害、マルチチャネルアナライザーの通信障害、そしてモーターコントロールユニット (MCU)[2] の通信障害、などである。

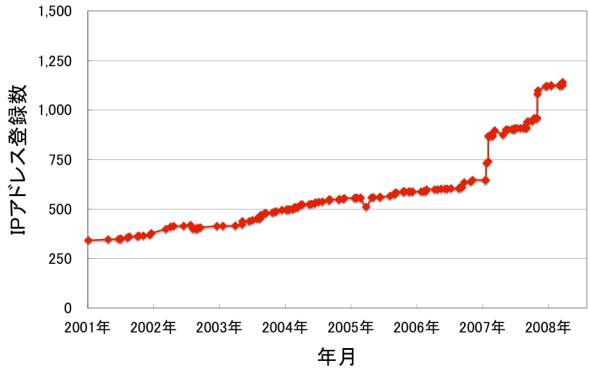

図 1: SPring-8制御系ネットワークにおけるIPアドレス登録機器数の変遷。2001年1月の342台から2008年3月の1141台まで3倍以上に増加している。

本研究の目的は、SPring-8加速器運転の安定性の向上である。運転に影響を与えている組み込み機器の原因を追及し、健全に運用するための改善を行う。今回特に通信障害を起こし、ネットワーク通信機能に脆弱性を有すると考えられる組み込み機器について調査を行った。

[1] E-mail: takashi.sugimoto@spring8.or.jp

２．研究の内容

加速器制御に使用する組み込み機器の通信機能について健全性・脆弱性を調査した。試験環境下において、機器に対し制御系ネットワークの通信に相当する疑似負荷を与え、機器の動作を確認した。通信負荷と機器の動作から、組み込み機器の脆弱性の原因を特定した。

前述した機器類のうち、本研究ではMCUについて調査を行った。MCUはSPring-8で開発し、CPUとOSにそれぞれSH4とNORTi4を使用した組み込み機器である。スリット・RF位相器および減衰器・ワイヤグリッドモニターの制御に利用され、SPring-8全体で20台が運用されている。MCUを選んだのは以下の理由からである; 1) SPring-8で開発した機器であるため、内部動作についての調査や改善も可能である, 2) 通信障害の発生頻度が他の機器より比較的高い（平均して1週間に1回程度）, 3) MCU通信異常の復旧のためにはSPring-8の入射加速器の停止と初期設定が必要となり、トップアップ運転の中断を引き起こす, 4) 制御系ネットワークの接続機器数・トラフィックと障害発生との相関が考えられる。特に4)に関し、MCUは2004年の導入以来安定して運用されていたが、2007年2月以降に機器障害が発生するようになった。2007年2月には接続機器が約200台増加しており、通信負荷増加に対するMCUの通信処理性能の不足が考えられる。現在までにMCUについて行った試験とその結果について以下で報告する。

2-1. 試験の方法

MCUの通信異常は、増加したネットワーク接続機器・通信負荷との相関が疑われる。MCUが持つイーサネットインターフェースの 1) 最大負荷性能、2) 連続負荷性能 について調査を行った。

2-2. 試験環境

図 2にネットワーク脆弱性試験ネットワークを示す。独立した試験用ネットワークを作成し、ネットワークスイッチ (HP ProCurve 2626-PWR) にMCU、VME計算機 (電産 DVE-686/50) 、疑似負荷印加用計算機 (IBM ThinkCentre S50) を接続した。またネットワークスイッチのモニタポートに通信監視用計算機 (Lenovo ThinkPad X61) を接続し、MCUの全通信を取得した。各機器とネットワークスイッチ間の接続速度は100 Mbps、全二重通信である。

2-2a. 最大負荷性能試験

疑似負荷印加用計算機からMCUに対して大量の通信を行い、MCUの応答を調べる。手法としてはBurst Pingを使用し、1秒あたり約2000パケットの送信レートでPing (ICMP echo-request) を送信し、MCUに応答 (ICMP echo-reply) させた。図 3に通信監視用計算機で取得したPing送受信パケットの時間変遷を示す。得られたデータより、MCUは以下のような通信機能の特性を持つことが判明した。

1. 受け取ったPingに対し、30 ms以内に応答を行う。これはリアルタイムOSとして要求される機能の一部である。
2. 30 ms以内にPing応答可能なパケット数上限は16個である。
3. MCUが30 ms以内に16個を超えるパケットを受信した場合、超過分はバッファされ、次の30 ms周期中に処理される。
4. 連続して超過した場合、バッファ溢れが発生し、処理できないパケットが発生する。

以上で得られた結果から、MCUが1秒あたりに処理可能なパケット数の理論上限値は1秒あたり533個であることが判明した。

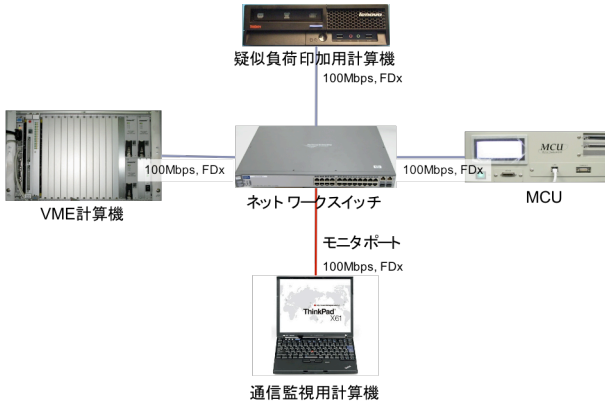

図 2: 脆弱性試験用ネットワーク。VME計算機, MCU以外に疑似負荷印加計算機, 通信監視用計算機を接続している。

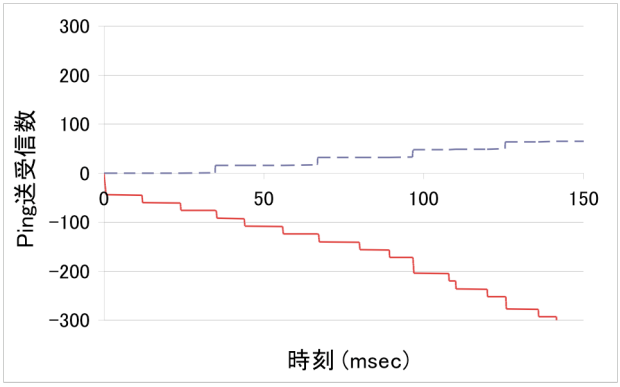

図 3: 最大負荷性能試験における、負荷印加計算機からのPing送信パケットとMCUからの応答パケットの時間変遷例。実線が送信パケット(負数)、破線が応答パケット(正数)を表す。

2-2b. 連続負荷性能試験

MCUに対して継続して通信負荷を与えた場合、前節で述べたバッファ溢れとパケット処理の欠落により、VME計算機間との通信異常が発生していることが疑われる。VME計算機とMCUが制御通信を行っている状態でMCUに通信負荷を与え、MCUの応答を調べた。手法としてSYN Floodingを使用した。負荷の印加に際しTCP通信要求(SYN)の送信レートを調整し、通信異常が発生する閾値を探した。得られたデータより、以下の結果が得られた。

1. 1秒あたり100パケット以下の連続的な通信負荷を与える場合、VME—MCU間の通信異常は発生しない。
2. 1秒あたり101パケット以上の連続的な通信負荷を与える場合、VME—MCU間の通信異常が発生する。

以上より、MCUが安定して連続処理可能なパケット数の上限は1秒あたり100個であることが判明した。

2-3. 試験結果と考察

最大負荷性能・連続負荷性能試験の結果から、MCUが安定して処理可能なパケットは1秒あたり最大100個であることが判明した。標準最大パケット長(1500 Bytes)の場合で1.2 Mbpsの帯域であり、MCUとネットワークスイッチ間の接続速度100 Mbpsに対して約100分の1に過ぎない。MCUは多量のネットワークトラフィックに対して脆弱であり、パケット処理能力不足がVME計算機との間の通信障害の原因と考えられる。

さらに、MCUへの通信負荷として本試験で使用したPingおよびSYNのユニキャスト（1対1通信）だけでなく、ブロードキャストパケットによっても通信障害を引き起こすことが判明した。TCP/IPの仕組み上、イーサネットインターフェースの物理アドレスとIPアドレスの対応付けにブロードキャスト（ARPパケット）が使用される。機器数の増加はMCUに対する通信負荷の増加に相関し、通信障害の発生頻度を高めている。また近年では動作環境としてWindowsを要求する機器が増加している。Windowsは名前解決にブロードキャスト（NetBIOS over TCP/IP：NBT）を使用するため、制御系ネットワークにおけるWindows計算機の増加も通信負荷を増やす一因となっている。

2-4. 機器障害への対策

以上で得られたような機器脆弱性の対策として、二通りのアプローチが考えられる。一つは機器自体の改善、もう一つはネットワーク通信環境の改善である。

2-4a. 機器の改善

MCUはSPring-8で開発した機器である。デジタルマルチメーターやオシロスコープ等の市販の機器と比べ、機器自体の改善を行うことは比較的容易であり、本アプローチによる改善を検討している。

条件が厳しい連続負荷性能の向上のために、フラッシュベースシステムからRAMベースシステムへの変更を検討している。一般にフラッシュメモリはRAMよりアクセス速度が遅く、フラッシュベースシステムではプログラム実行速度を決める要因となりうる。現在RAMベースシステムによる動作試験を進めており、主にキャッシュの効果により連続負荷性能の向上を見込めることが明らかになってきている。

一方で最大負荷性能はRAMベースシステムでも向上していない。比較のためMCUのハードウェア上で他のOS (SH-Linux) を動作させた場合、Burst Pingに対する応答ロスは発生していない。すなわち、MCUの最大負荷性能はハードウェアでなくOSとそのプロトコルスタックで決定されており、現在使用しているOSでは通信性能が十分に発揮できていないことを示している。OSを含めたソフトウェアの変更も選択肢に入れ、機器の改善を検討中である。

2-4b. ネットワーク通信環境の改善

機器自体の改善が困難な場合、通信環境の改善による対策が必要となる。MCUの場合も、前述のRAMベースシステムへの変更はまだ完了しておらず、平行して通信環境の改善による対策も行う。方法としては、ブロードキャスト到達範囲の分割とパケットフィルタを検討している。

SPring-8の制御系ネットワークは、全加速器を一つのネットワークセグメントに収容するため、マスク値21bit（2048アドレス）で構成されている。セグメント内で発生したブロードキャストは全ての機器に到達し通信負荷となる。定常運転時のブロードキャストは毎秒15パケット程度であるが、機器の動作状況により増加し、通信異常の要因となっていると考えられる。ブロードキャスト到達範囲を分割することにより、通信負荷が減ることが見込まれる。さらに、組み込み機器の動作に不要なパケット(NBT等) をフィルタすることにより、通信負荷をより減らすことが可能になる。

以上で述べた改善案のうち、可能なものから今秋の運転サイクルから試行する。MCUの動作の健全化を図ることで、加速器運転の安定性の向上を目指す。

まとめ

SPring-8では多数のイーサネット対応組み込み機器を使用し、加速器の状態計測・制御を行っている。しかしながら、組み込み機器の一部は通信障害を発生し、加速器の運転に影響を与えている。本研究では、加速器制御に使用される組み込み機器のネットワーク通信に関する脆弱性を調査した。

SPring-8で開発し、運用を行っているモーターコントロールユニットについて調査した結果、パケット処理能力の不足が通信障害を発生させる原因であることが判明した。加速器運転の安定性を向上させるため、機器自体の改善と通信環境の改善を検討し、試行する予定である。

また、MCU以外で障害が発生しているデジタルマルチメーター、オシロスコープ、マルチチャネルアナライザーについても今後詳細な調査を行う予定である。

[1] T. Fukui et. al, Proceedings of ICALEPCS'01, THDT005 (2002).
[2] T. Masuda et. al, Proceedings of PCaPAC2005, WEP30 (2005).