審 査 の 結 果 の 要 旨

氏　　名　　岡部　宣夫

本論文は、「大規模産業システムにおけるSecure Plug and Playアーキテクチャに関する研究」(英訳：A Study on Secure Plug and Play Architecture for Large Scale Industrial Systems)と題し、大規模な産業システムに対して、その技術課題と新しいシステム展開の考察と検討を行い、最新のオープンネットワーク技術の適用と、オープンネットワーク技術を適用しながらもグローバル規模の大規模システムにおいて、十分なセキュリティ機能をプラグアンドプレイに提供することを可能とするシステムアーキテクチャの検討ならびに提案、さらに、提案アーキテクチャを実現するために必要なコンポーネント技術の提案とその実装、さらに、それらの動作検証と性能評価を行っている。 本論文は、8章から成り立っており、グローバル規模で運用される大規模産業システムの要求条件を、オープンコンピュータネットワークの観点から整理し、さらに、オープンシステムの導入に伴い新たに発生するシステム上の問題および課題を明確化し、必要となるコンポーネント機能に関する具体的な要求条件の整理とそのフレームワークの提案を行い、さらに、システム全体のアーキテクチャの提案を行っている。 また、オープンシステムの導入による、これまでの大規模産業システムに対する利点を明確化、その具体的な適用手法を提案している。また、産業システムに必須となるセキュリティ機能の実現を、自律的な動作環境で、かつ低コストに実現し、さらに、運用管理コストの削減の観点から必須とされるプラグアンドプレイ機能を組み込むことを可能とするシステムアーキテクチャを提案している。 提案システムの試作とその評価を行い、提案システムの有効生を示すことに成功している。

第1章と第2章において、本研究の目的と対象である産業システムの概要とその典型的システムのシステム規模と構成を概説している。産業システムとは、Process AutomationやFactory Automationなどに代表される制御システムであり、製造業やエネルギー産業や交通機関のように、社会基盤としての責任を担っている。システム要素の障害は、社会や企業に対して莫大な被害や影響を与えるため、システムには高度な信頼性が要求される。システムのライフサイクルは長く、いわゆる枯れた技術も多く使われる。システムの末端部分はフィールド領域と呼ばれ、センサーやアクチュエータなどの多様なフィールドデバイスから構成され、固有の技術が用いられる。これに対して、上位のシステム領域では、IP（Internet Protocol）技術が主流である。現在の大規模な産業システムのフィールド領域は、数百のコントローラと数万のフィールドデバイスから構成され、その規模は、さらに大きくなることが予想されていることを議論している。

第3章では、現在の産業システムが抱える課題を検討整理、以下の6つ技術課題を解決しなければならないことを示している。(1)グローバルスケールでの生産の効率化を実現に資する技術的にフラットなシステム構成。(2)ダウンタイムの削減を実現するための高度なシステム観測技術と障害復旧技術。(3) 新しい応用を創出作するための最新の通信技術の導入を可能とするアダプタビリティ。(4) 最新のデータリンク技術による経済的なワイヤリング技術。(5)設定作業の自動化によるエンジニアリング作業の負担軽減技術。(6)フィールド領域にも適用可能な安価で安全な通信セキュリティ技術。

第４章では、関連研究として、産業用イーサネット、Plug and Playに関連した研究、end-to-endセキュリティ機構について議論し、既存研究では上記の課題が解決できないことを示している。

第5章では、上述した課題を解決するためのアーキテクチャをとして以下の3つの特徴を持つシステムの提案を行っている。１）フィールド領域のネットワーク化は、フィールド領域が多様なデータリンク技術を導入することを可能にする。システム全体の通信基盤技術を統一することは、技術的にフラットなシステムを意味し、システムをcontroller-centric モデルから脱却させ、システムの分散化と高機能化を容易にする。２）フィールドデバイスに適したセキュリティアーキテクチャは、分散システムに必須なネットワークのセキュリティを実現する。通信のセキュリティにはIPsecを利用するが、その鍵交換には新しい方式を提案することにより、計算資源の制約されたフィールドデバイスなどのネットワーク機器にも適用可能となる。この鍵交換プロトコルを普及させるために、IETFにおいてRFC4430として国際標準化を行った。３）フィールドデバイスに適したSecure Plug and Playアーキテクチャは、フィールドデバイスなどのネットワーク機器に対して、設定作業の自動化と故障からの復旧支援を提供する。これは、上述したセキュリティアーキテクチャに基づくため、計算能力の限定されたネットワーク機器が適用できるセキュリティを備えている。

第6章では、提案するアーキテクチャの試作と評価を行っている。試作システムは、組込み用途のCPUを用いた試作ドデバイスと既存のPCを利用したサーバ群から構成される。試作デバイスの性能評価の結果、実運用に必要な性能を実現可能であることを確認することができた。ノードの全オブジェクト（リアルタイムOSやIPスタックを含む）は272kbytesであったが、Plug and Play部分は16kbytesで実現することに成功しており、コンパクトな実装が可能なアーキテクチャであることを示した。試作システムのサーバの性能に関して、Kerberosのトランザクション処理時間は1ミリ秒以下と十分な性能を実現していることを確認することができた。(独自仕様の)データベースとのトランザクション処理には改善の余地が見出されたが、一般的なデータベースを用いれば、性能を改善できると期待される。さらに、本研究では、種々の実証実験と通じて、異なるプラットフォームへの移植性や実環境下への適用性も確認することができた。起動中の機器に対するセキュリティを考慮したPlug and Play機能、計算コストの低いセキュリティアーキテクチャ、さらに拡張性と暗号アルゴリズムのポータビリティー性に優れるアーキテクチャは、産業システム以外の応用領域においても適用可能であり、かつ有用である。

第7章では、今後の研究課題を明らかにしている。第一は、防爆環境に適したより高性能なデータリンク技術の検討である。通信帯域の向上、パケットの優先処理、DoS対策が今後の研究課題である。第二は、大規模な分散システムに適したKerberosの拡張である。大規模な分散システムに Kerberos を適用するなら、複数の管理領域に跨がった認証を想定し、以下の課題を解かねばならない。(1)途中のKerberosサーバが故障すると、最終的な認証が失敗するという脆弱性への対処。(2)認証に必要なメッセージが、Kerberosのサーバ数に比例して増加してしまう。(3)メッセージ処理をホストが負担せねばならないため、計算資源の制約されたノードでは実現が困難となる。

最後に、第８章では、「まとめ」として,本論文での議論の総括と,今後の課題について述べている.

本論文では、グローバル規模で動作する大規模産業システムに対して、その技術課題の考察と検討を行い、最新のオープンネットワーク技術を適用しながらもグローバル規模で十分なセキュリティ機能をプラグアンドプレイに提供することを可能とするシステムアーキテクチャを提案、試作システムの設計と実装、さらに、それらの動作検証と性能評価を行っており、その有用性は高く評価できる。

以上のように、本論文は、情報システムアーキテクチャにおける実用性の高い結果を示しており、情報理工学における創造的実践に関して高い価値が認められる。よって、本論文は博士(情報理工学)の学位論文として合格と認められる。