論文の内容の要旨

論文題目　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

氏　名　　岡部　宣夫

本研究の対象は、大規模な産業システムに対して、最新のネットワーク技術を適用することで、現在のシステムが直面している課題を解決することである。

産業システムとは、PA (Process Automation)や FA (Factory Automation)などに代表される制御システムである。この分野のシステムは、石油精製や製造ライン等の製造業、電力などのエネルギー産業、電車などの交通機関のように、社会基盤を担っている。一度故障すると莫大な被害や社会的な影響を与えるため、システムには信頼性が重視され、システムのライフサイクルは長く、5 年から 20 年は動き続ける。このため、システムには、いわゆる枯れた技術が多く使われる。例えば、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ている。フィールド領域より上位では IP (Internet Protocol)技術が主流であるが、フィールド領域は独自の技術が使われている。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る。

現在の産業システムが抱える主な課題は以下である。第一に、グローバルスケールでの生産の効率化を実現するためには、技術的にフラットなシステムが必要である。第二に、ダウンタイムを削減するため、システムの観測技術の強化と故障からの復旧を支援するための技術が必要である。第三に、新しい通信技術の導入の容易性にすることで、新しい応用を作り出すこと。第四に、最新のデータリンク技術を活用することで経済的なワイヤリングコストを実現すること。第五に、設定作業を自動化することで、エンジニアリング作業の負担を減らすこと。第六に、フィールド領域をもカバーできる通信のセキュリティを実現すること。

本研究では、これらの課題を解決するために、下記 3 つ提案を行った。

１）フィールド領域の IP ネットワーク化：
　これにより、フィールド領域は、多様なデータリンク技術を導入することが可能とな

2）フィールドデバイスに適したネットワークセキュリティアーキテクチャ：
これにより、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。具体的には、IPsec を利用するが、鍵交換には従来の IKE ではなく、Kerberos を利用した新しいものを提案する。このセキュリティアーキテクチャは、一般の計算機だけではなく、フィールドデバイスなど計算資源の制約されたノードにも適用可能である。また、この鍵交換プロトコルは、IETF において RFC4430 として国際標準化された。

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：
これにより、フィールドデバイスなどの機器に対して、設定作業の自動化と故障からの復旧支援を提供できる。このアーキテクチャは、計算資源の限定されたノードでも適応可能なセキュリティを備えている。

本研究では、提案するアーキテクチャの試作と評価を行った。試作システムは、組込み用途の CPU を用いて、擬似フィールドデバイスとしてのノードと既存の PC を利用したサーバ群から構成される。ノード側での性能は、Plug and Play の処理に 793m 秒、デバイス間通信で IPsec を確立するための処理に 290m 秒を要した。これらの処理は、主に立ち上げ時に発生するので、性能上の問題はないと考える。また、長期間の運用では、IPsec の鍵交換（65m 秒程度）が発生する。しかし、鍵の有効期限を調整することにより、鍵交換の発生頻度を調整できる。また、IP プロトコルスタック内での受信パケット処理に優先順位を導入することで、制御パケット処理への影響を小さくすることも考えられる。ノードの全オブジェクトは 272K バイトで、Plug and Play 部分は 16K バイトで実現できたことにより、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側の性能に関しては、Kerberos のトランザクション処理時間は、646 μ 秒から 782 μ 秒と十分に速かったが、PS のトランザクションよりは 100m 秒と遅かった。本アーキテクチャは特定のデータベース技術を仮定していないので、一般的なデータベースを用いれば、性能を改善できると考える。サーバのスケーラビリティに関しては、DHCP と NTP の対策は容易であるが、Kerberos と PS のは、今後の研究課題であった。更に、試作などを通じて、サーバのセキュリティに関する考察も行った。

本研究では、実証実験も実施した。牛肉のトレーサビリティシステムに Secure Plug and Play の試作システムを適用することにより、センサーシステムの設定を自動化に貢献した。この実証実験を通じて、異なるプラットフォームへの移植性や実環境下での機能を確認した。

今後の研究課題は二つある。最初の研究課題は、防爆環境に適したデータリンク技術の検討である。産業システムの特定分野では、爆発危険性ガス、可燃性粉塵、繊維くずなど爆発などの可能性のある環境が存在する。この様な環境下でシステムを制御する場合には、該当する部分の機器が爆発や火災の原因となることを防ぐために、防爆規格という規制に従わねばならない。本研究では、このような環境下で IP パケットを搬送するデータリンクを試作したが、その性能は十分ではない。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。次も研究課題は、大規模な分散システムたいする Kerberos の拡張である。大規模な分散システムに Kerberos を適用すると、複数の管理領域に跨がった認証が発生する可能性がある。この場合、以下の課題を解決せねばならない。1）Kerberos サーバ間の信頼関係のモデルでは、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がある。 2）認証に必要なメッセージが、Kerberos サーバ数に比例して増加するのはスケーラビリティ上の制約である。 3）これらの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である。これらの Kerberos 拡張に関して、IETF で標準化活動を実施している。

本研究で提案した技術は、大規模な産業システムを想定しているが、一般的なシステムにも適用可能である。まず、本アーキテクチャは、IP、IPsec、Kerberos など、標準的なネットワーク技術に基づいている。次に、本研究で考慮したノードの制約条件（計算能力や消費電力など）は、産業システム以外の分野にも該当する。また、近年サーバ側の性能や発熱が問題を考慮すると、サーバ側の負荷軽減という観点からも、計算量の小さいセキュリティアーキテクチャは有用である。