M-15

耐改ざん性を考慮した生産管理情報蓄積装置へのデータアクセス手法の検討

Data Access to Production Management Information Storage Device Considering Tamper Resistant

○山中響[1]，　望月寛[2]，　中村英夫[3]
* Hibiki Yamanaka[1], Hiroshi Mochiduki[2], Hideo Nakamura[3]

Abstract: Traceability is required for products that are shipped from industrial field. Therefore production management information that is recorded when manufacturing is so important. In this paper, we studied architecture of a product management information storage device with the protection against data falsification and aimed to develop using FPGA. Specifically we proposed configuration methods in which the optimized commands for data requirement and access control using reconfigurable component are included.

１．はじめに

市場に出荷されている製品には流通経路などのトレーサビリティが求められており，生産現場に対しては，製品製造時に発生する生産管理情報の管理が重要視されている。生産管理情報は製品が市場に出荷され，万が一不備があった場合に製品製造時における問題の有無に使用される[1] [2]。図 1 に生産管理情報蓄積装置を用いたシステム構成を示す。近年，生産現場のセンサの高速化・高信頼化により「抜き取り検査」から製品すべてを検査する「全数量検査」が可能となり，計測値のリアルタイム処理・保存がボトルネックとなっている。現在では生産管理情報の保存に PLC（Programmable Logic Controller）内部のメモリを使用しており 1 日分のデータしか確保できないため，毎日のデータをプリンタに出力し，紙データとして保管している。そして，紙データは容量の増加に伴い保存場所の確保が難しくなるうえに経年劣化もする問題がある。さらに，通常の情報機器によるデータログ環境を用いていることにより，容易に生産管理情報を改ざんでき，製造段階での問題が確認できない可能性がある。そこで，10 年といった長い期間のデータの記録及びシステムの動作保障が実現できる高信頼な生産管理情報蓄積装置が求められている。システムは主に GOT（Graphic Operation Terminal）で操作を行い，生産ライン上で発生した生産管理情報は生産管理情報蓄積装置において管理・保存を行う。生産管理情報を蓄積装置に保存する場合には，データの改ざんを不可能とするほか，暗号化処理を施しデータの漏洩を防止する。また，ユーザーID とパスワードを入力することで，USB メモリに生産管理情報の出力可能な構成となっている[3]。

以上を踏まえて本研究では，耐改ざん性に配慮した生産管理情報蓄積装置の構成について検討した。特に，生産管理情報へアクセスするためのコマンドの最適化，及びリコンフィギャラブルなデバイスを用いたストレージ用 CPU へのアクセス制限手法を提案し，プログラマブルなデバイスである FPGA を用いた実装を試みる。

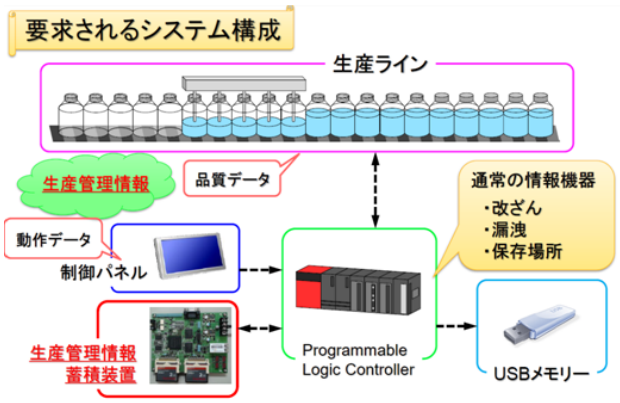

Figure 1. System requirement for a product management information storage device.

２．生産管理情報蓄積装置の要件と方策

生産管理情報蓄積装置に必要なシステムは重要な生産管理情報が漏洩しないセキュリティ，情報の欠落を許容しないデータの完全性，プロセッサ自身の高信頼化，意図的に情報を書き換えることのできない耐改ざん性の 4 点である。データ記録用媒体として，高信頼化を図るために HDD 等機械的な構造を有しない装置とする。そのため，耐久性に優れているコンパクト・フラッシュメモリを採用し，さらにソフトウェアによるメモリカードの二重化を行うことにより，長時間の安定稼動を実現する。優先度制御タスクは停止タスクの優先度を一時的に高くすることで停止タスクを起動し，停止時間の最悪値を保証している。これにより，例えば書込み処理に時間がかかりデータ受信処理が起動しないといった問題を回避することができる。

１：日大理工・院・電子　２：日大理工・教員・情報　３：日大理工・教員・電子

３．不正操作などによるデータ改ざんの防止策

図 2 に示すようにストレージ制御用 CPU とアプリケーション用 CPU とを RAM を介する構成とし，物理的に切り分けることでユーザプログラムから保存メディアのアドレスを直接参照できない仕組みとした。さらにデータ書込み時のアドレスを自由に監視・制御できるミドルウェアを作成し，同一アドレスへの書込み制限機能を実現することができた。

図 3 にはコマンドの最適化によってユーザプログラムからのデータ改ざんを防止する構成を示す。この図より，図 2 と同様に RAM を介することによってストレージ制御用 CPU とアプリケーション用 CPU とを物理的に分離する構成をとっている。そして，リモートサーバおよびリモートコマンドを用いて各 CPU 間の通信を行う。これにより，アプリケーションからディスクのアドレスに対する直接参照を制限することができるため，アプリケーション層で不正に実行されたプログラムや誤動作などによるデータの上書き・破壊を防ぐことができる。それに加えて，図 3 の方式においては，常にコントローラからアプリケーションに対して，生産管理日時などの情報をアプリケーション用 CPU に対して送信する構成を採用する。そしてユーザプログラムによって情報が必要であると判断した場合のみ，データ要求コマンドを送信し RAM との通信を可能とする。この利点は，コントローラをマスタに固定し，アプリケーション用 CPU からは最低限の要求コマンドしか送れないため，データ改ざんを行うことが困難となる。一方，図 4 にリコンフィギャラブルなデバイスを用いてアプリケーション用 CPU からのアクセスを制限することによってデータ改ざんを防止する構成を示す。この図より，アプリケーション用 CPU と RAM の間に FPGA などのリコンフィギャラブルなデバイスで構成された RAM を用意しておき，認証が終わるまでは認証回路と RAM 内との配線を分離する構成とした。この利点は，認証回路が認証するまで RAM との通信が行えないことから，ストレージ制御用 CPU に対して不要なコマンドが送信されないという点が挙げられる。

４．まとめ

本研究では，耐改ざん性に考慮した生産管理情報蓄積装置について，コマンドの最適化およびリコンフィギャラブルなデバイスの採用した構成を検討した。現在，これらの提案手法に基づいて実際に FPGA を用いた開発を行っており，今後，それの性能評価を行うことによって研究の深度化を図りたい。

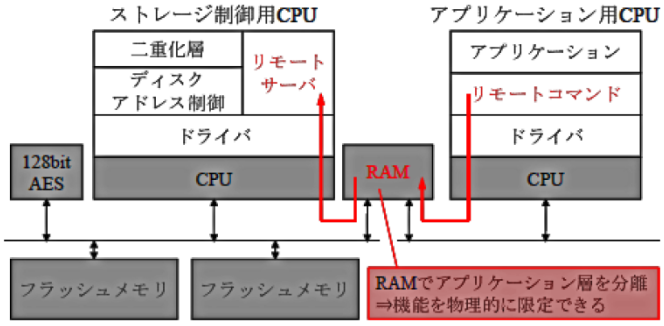

Figure 2. Architecture of the protection against data falsification.

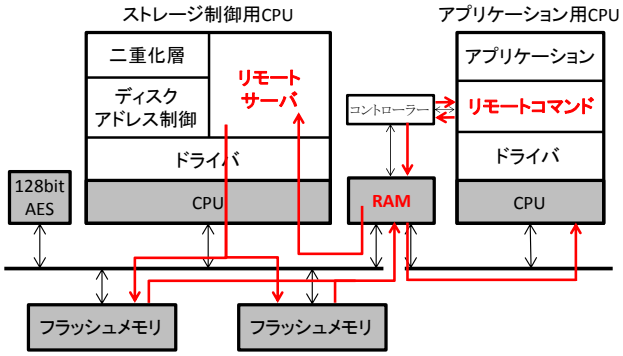

Figure 3. Configuration with the optimized commands.

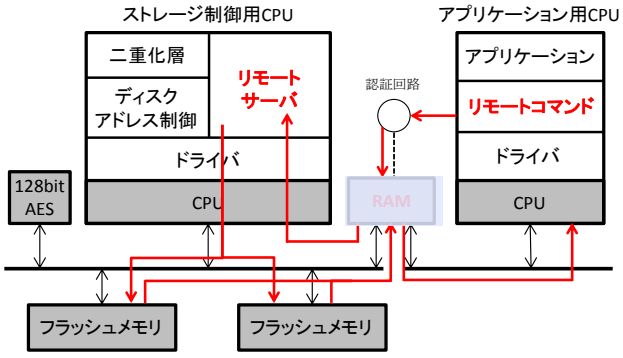

Figure 4. Configuration with a reconfigurable device.

５．参考文献

[1] J. G. Campos and M. Hardwickb, “A traceability information model for CNC manufacturing ”, Computer-Aided Design, Vol. 38, pp. 540－551 (2006).

[2] A. Adamyan and D. He : “Analysis of sequential failures for assessment of reliability and safety of manufacturing systems”, Reliability Engineering and System Safety, Vol. 76, pp. 227－236 (2002)

[3] 太田他，“ディペンダブルな生産管理情報蓄積装置に関する一検討”，信学技報，Vol.110，No.333，pp.5-8 (2010).