M-26

耐改ざん性を考慮した生産管理情報蓄積装置の設計

Design of dependable data logger for inline production management considering data falsification protection

○山中響 [1]，小川雄也 [2]，望月寛 [3]，中村英夫 [3]
*Hibiki Yamanaka[1], Yuya Ogawa[2], Hiroshi Mochizuki[3], Hideo Nakamura[3]

Abstract: We have studied an architecture of protection against data falsification, integrity of the collected data, security against data leakage, and the implementation for FPGA on dependable data logger for inline production management. This data logger records production management data in product manufacturing. This management data is important so that problems at the manufacturing stage can be traced when problems are reported after shipping. In this paper, we consider monitoring function for protection against data falsification. Specifically we designed a method to access data of compact flash memories via RAM.

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．Fig. 1 に示した生産管理情報蓄積装置を用いたシステム構成によると，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 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．

以上の背景より，本研究では生産ライン上で発生した生産管理情報高信頼で保存する生産管理情報蓄積装置の開発を目的とし，特に耐改ざん性を考慮したデータアクセス機構を設計したので報告する．

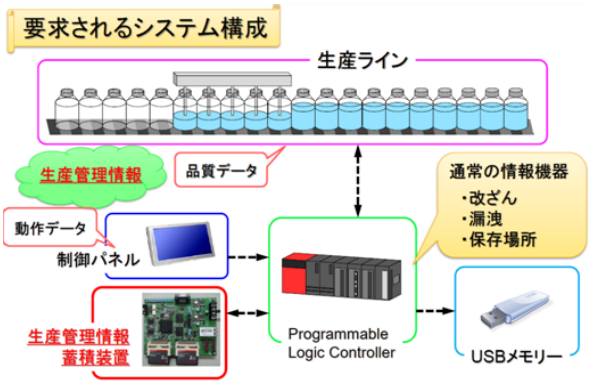

Figure 1. System requirement for traceability.

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．なお，データ記録用媒体として，高信頼化を図るために HDD 等の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．以上の要件を踏まえて，現在までに実施した研究では，プロセッサ自身の高信頼化を目的として Hot Standby 方式を用いた 3 重系の回路構成を提案した [1][2]．その構成を Fig. 2 に示す．各々の CPU は同一のクロックで同じ処理を行い，その動作を 3 つの照合回路により監視を行う．その結果，割込み

1：日大理工・院（前）・電子　2：日大理工・院（前）・情報　3：日大理工・教員・子情

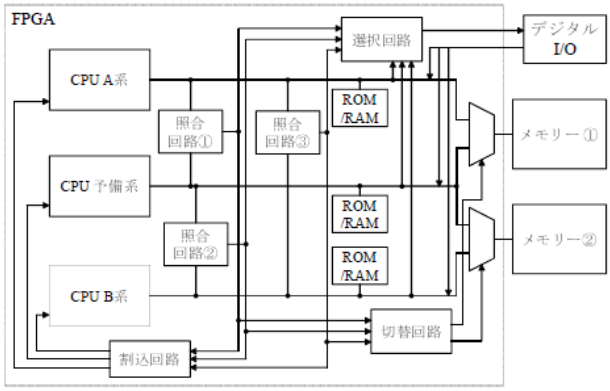

Figure 2. Reliable CPU system using a hot-standby method.

回路では，故障と判断される系への割込みを行う．また，切替回路では 2 つの正常な系を選択する．正常な場合の 3 つの CPU と 2 つのメモリーの接続は，A 系がメモリー A に，B 系がメモリー A にデータを書き込む．読み込み時は，A 系と予備系がメモリー A，B 系はメモリー A のデータとなる．そして，デジタル I/O 等の出力が 1 つなものに対して，3 つの CPU から正常な 1 つを選択し出力を行う構成となる．故障と判断された系は故障診断を行い，残りの正常な系での動作を継続する．また故障診断の結果，故障箇所が判断できない場合には一過性の誤りとみなし，チェックポイントに戻り元の正常な動作を継続する．

3. 不正操作等によるデータ改ざんの防止策と設計

ストレージ制御用 CPU とユーザプログラム実行用 CPU 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．Fig. 3 にユーザプログラムからのデータ破壊防止のアーキテクチャを Fig. 4 にはユーザプログラムからのデータ破壊防止の RAM への書き込み構成を示す．RAM を介することによって，ストレージ制御用 CPU と，ユーザプログラム実行用の CPU を物理的に分離している．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等によるデータの上書き・破壊を防ぐことができる．

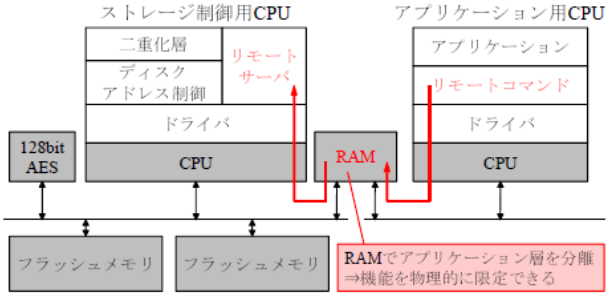

Figure 3. Architecture of function isolation using RAM.

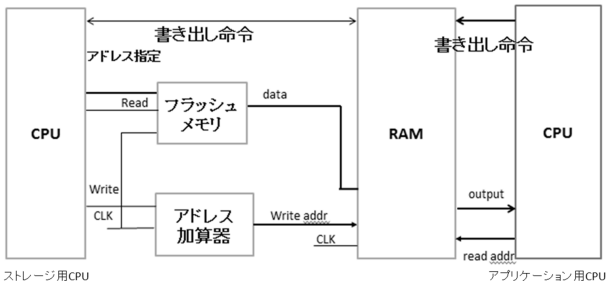

Figure 4. Detailed design of writing composition for data falsification protection.

4. まとめと今後の課題

製品製造時に発生する生産管理情報を管理するため高信頼な生産管理情報蓄積装置について，その要件をまとめた上で，特に耐改ざん性に対する具体的な方策を示した．具体的にはストレージ制御プログラムとユーザプログラム用のアドレス空間を RAM を介すことで，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ができることを明らかにした．

現在，この設計に基づいて FPGA を用いた実装を行っており，今後，開発した機構の性能評価を実施したいと考えている．

参考文献

[1] K.SAKAMAKI et. al. DESIGN OF DEPENDABLE DATA LOGGER FOR INLINE PRODUCTION MANAGEMENT ; The 4th Asia-Pacific International Symposium on Advanced Reliability and Maintenance Modeling, Vol. 4, No. 1, pp. 580-587 (2010).

[2] 太田匡哉 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).