論　文

高信頼なインライン計測システムのためのストレージアーキテクチャ

金田　泰昌*1)　　入月　康晴*1)　　佐野　宏靖*2)

Storage Architecture for a Dependable In-line Measurement System

Yasuaki Kaneda*1)，Yasuharu Irizuki*1)，Hiroyasu Sano*2)

Recently, information technologies are often used in field instruments. The reason is that efficient production and In-line measurements for which both production and measurement are performed in the same line will become possible. However, there is a problem that digital data obtained in a field can be tampered with very easily. A major solution to this problem is connecting the data management system to field instruments via a network. But in some cases, it may not be possible to connect field instruments to a network because of security. Accordingly we aim to develop a stand-alone embedded instrument that can obtain and manage data in the field, and have studied the necessary architecture. As a result, we achieved a mirroring system using FPGA and flash memory that can write data at the rate of about 26KByte/s and improve the availability of instruments. By using a watchdog timer, a new mechanism is proposed such that the data receiving process can restart as soon as possible in the event it stops. In the experiment, it is demonstrated that the constructed system can receive and manage data sent at 64Byte each 100 millisecond without fault.

キーワード：インライン計測，信頼性，ストレージ

Keywords：In-line measurement, dependability, storage

1.　はじめに

近年，生産設備の IT 化が進められている。その背景として，生産情報の電子化により生産の効率化が行えることが挙げられる。また，センサの高速化・高精度化・低価格化により同一ライン上で生産と計測を行う「インライン計測」が可能となってきており，その結果として効率的に製品のトレーサビリティを確保することが可能となってきていることも背景として挙げられる。

このように電子データを用いることで様々なメリットが得られる反面，電子化された情報を改ざんし，商品の品質を偽装する問題が多発している。たとえ電子データを生産ラインの中で計測・記録できたとしても，そのデータの信頼性が保証されなければトレーサビリティの保証にはならない。このような問題から，様々な業界で電子データの信頼性確保について感心を寄せており，各業界で電子データの取り扱いについての規約を定める活動が始まっている。例えば製薬業界では， FDA （Food and Drug Administration : アメリカ食品医薬品局） が電子データに対する取り決めとして 21 CFR Part11[(1)]を定義しており，また日本では厚生労働省が平成 17 年 4 月 1 日に FDA 21 CFR Part11 をベースとした「医薬品等の承認又は許可等に係る申請等における電磁的記録及び電子署名の利用について」という通達（薬食発第 0401022 号）[(2)]を出している。

電子データの信頼性確保に関する技術的な解決方法としては，物理的に 1 回しか書込めない（WORM : Write Once Read Many）メディアをマスタデータの保存に用いることで, マスタデータの改ざんを防止するものがある[(3)]。しかし，大容量の WORM メディアは高価であり，大量の生産情報を保存するメディアとしては不適切である。また生産設備とストレージサーバとをネットワークで接続し，データ管理システムを構築する方法がある。しかし，例えば屋外でデータを取得する場合等，データの取得現場の状況によってはネットワークに接続出来ないケースがある。またセキュリティ等の理由で機器をネットワークに接続したくないケースも存在する。さらに，ストレージサーバを導入することで，サーバ設置に伴うコストやサーバメンテナンスにかかるコストが非常に高くなる問題もある。

一方，ネットワークに接続出来ない飛行機や車の事故原因等を追跡する目的で，フライトレコーダーやドライブレコーダーと呼ばれる，運転履歴データ等を記録・管理する装置が存在する。これらと同様に，生産現場にも専用のデータロガーが存在すれば，ネットワークを介すことなく生産情報を保存・管理することが可能となる。

そこで本研究ではネットワークに接続出来ない生産設備において，そこで得られた電子データの品質を保証するために，スタンドアロンで生産情報を高信頼に保存・管理することが出来るストレージ機器を開発することを目指す。

*1) 情報技術グループ
*2) 電子・機械グループ

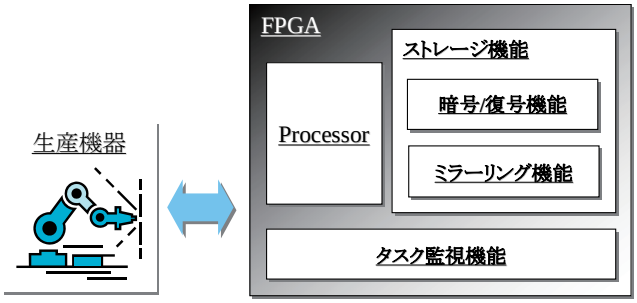

図 1. システムの概略

2. システムの要件と方針

スタンドアロンで生産情報を高信頼に保存・管理する組込み機器に求められる要求事項を整理すると以下の 3 つの項目になる。

(1) 不正操作等によるデータ改ざん防止機能の実現

データの品質を保証するために，記録された生産情報が改ざん出来ないことが必要条件となる。そこで，ストレージ部分の機能を他機能から分離し，外部からはストレージのアドレスを直接参照できない構成を採用する。これにより，不正なアクセスやプログラムの暴走によるデータの改ざんを防ぐことが出来る。

(2) 大容量データの長時間安定記憶の表現　　生産設備は 24 時間稼動することもあるため，長時間にわたり安定的に，かつ取りこぼし無くデータを記録する必要がある。そこでミラーリングを用いて，システムの可用性を向上させる。さらに，処理の動作状態を監視することで，万が一処理が停止したとしても素早く復帰できる手法を検討する。

(3) 盗難時のデータ読出し防止機能の実現　　スタンドアロンでの使用を前提としているため，万が一の盗難等によるデータの読出しを防ぎ，データの流出を防止する必要がある。そこで，データの暗号化を採り入れる。ここでは，

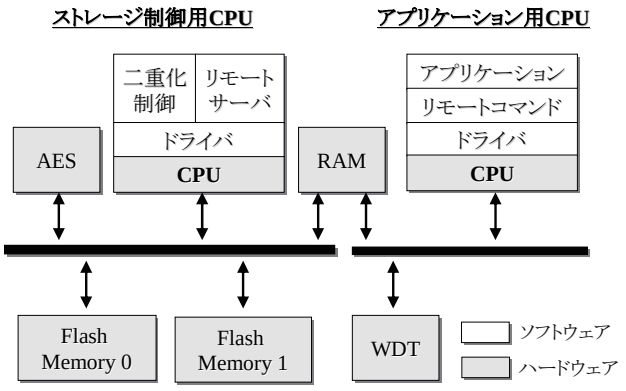

図 2. システムの全体構成

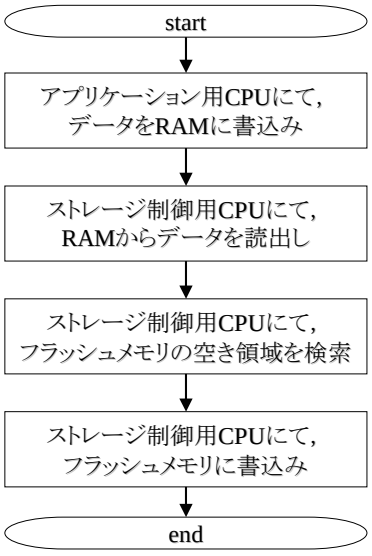

図 3. 書込みフロー

生産性を妨げることなく暗号化を実行する手法について検討する。

以上の 3 項目を採り入れたシステムの概略を図 1に示す。なお本研究では FPGA を用いて実装・評価を行う。

3. 実現手法

3. 1 全体構成　　システムを構成する主要なパーツを図 に示す。次節からは，2章で挙げた 3 つの項目について主要パーツと対応させながら説明する。

3. 2 データ改ざん防止機能の実現手法　　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 との間に RAM を介して接続しており，二つの機能を物理的に分離している。そして各 CPU 間の通信はリモートサーバおよびリモートコマンドを用いて行う。これによりアプリケーション側からフラッシュメモリのアドレスを直接参照出来ない仕組みとすることが出来る。

アプリケーション用 CPU からデータを書き込むためには，アプリケーションから書き込みたいデータを RAM に書き込むと，ストレージ制御用 CPU は RAM にあるデータを取得した後，フラッシュメモリの空き領域を検索し，空き領域にデータを書き込む。このように，一度書き込まれたデータ領域を上書きしないことで，データの改ざんを防いでいる。以上の書込みのフローを図 3 に示す。また，アプリケーション用 CPU からデータを読み出す際は，読み出したいデータのインデックスを RAM に書き込むことで，それに対応したデータをストレージ制御用 CPU が検索し，アプリケーションに返す。なおデータを書き込む際に，フラッシュメモリにデータのインデックステーブルも同時に構築しておくことで，読出し時の検索効率を向上させることも可能である。

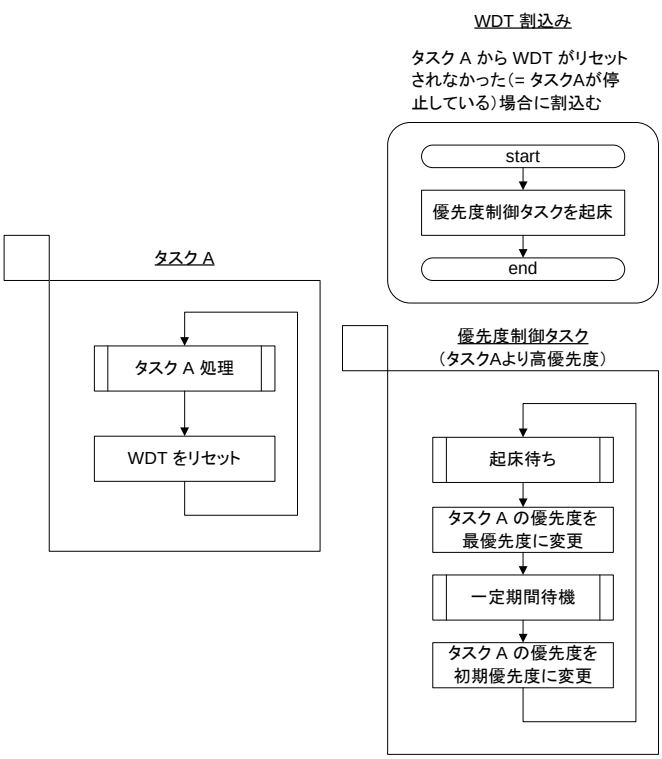

図 4. タスク停止を検出・復帰するための機構

3. 3　大容量長期間記憶の実現手法　図 4 に示すような本ミラーリング方式では，ソフトウェア的にメモリの二重化制御を行っている。また二重化制御では，①データ書込み制御，②データ読出し制御，③ホットスワップ，④自動リカバリ，の 4 つの機能をサポートしている。さらに，耐久性に優れ，近年大容量化・低コスト化が進んでいるフラッシュメモリを採用することで，ハードウェア的にも長時間の安定稼動を実現している。

本研究で構築したシステムはマルチタスクシステムであり，様々なタスクが切り替わりながら動作している。そのため，一つの処理が長時間実行されていると，他の処理が実行できなくなってしまう（停止してしまう）。例えば，受信タスクと書込みタスクの二つのタスクが存在した場合，書込みに処理時間がかかってしまうとデータ受信タスクが実行することが出来ず，最悪の場合データを取りこぼしてしまう恐れがある。

そのためストレージ制御部での処理の停止を検出・復帰するための機構を，タスク A を例として，図 4 に示す。タスク A では処理を行う度に WDT （ウォッチドッグタイマ） のリセットを行うようにしておく。これにより，タスク A が何らかの理由で処理が停止してしまうと WDT がリセットされず WDT の割込みがかかる。WDT 割込みが発生するとタスク A が停止していると判断し，強制的にタスク A の優先度を変更するための処理（優先度制御タスク）を起動する。ただし，優先度制御タスクは全タスクの中で一番優先度が高いとする。そして，優先度先行タスクからタスク A の優先度を一時的に高くすることで処理の停止を防ぐ仕組みにしている。

offset	register name	31	2	1	0
+0	Control		data set mode	mode	start
+1	Data0	Data [31..0]			
+2	Data1	Data [63..32]			
+3	Data2	Data [95..64]			
+4	Data3	Data [127..96]			

図 5. 暗号化ハードウェアのレジスタマップ

表 1. コントロールレジスタの詳細

Bit	Specifications
start　(R/W)	(書込み時)　1 : Start (読込み時)　1 : Execute　0 : Stop
mode (R/W)	1 : 復号化　0 : 暗号化
data set mode (R/W)	1 : データレジスタは鍵 0 : データレジスタは平文

3. 4　データ読出し防止機能の実現手法　本システムでは，信頼性の観点から，世界的に標準でありかつ実績のある暗号方式である AES を採用することを考えた。ただし，組込み機器の場合処理能力が PC よりも劣るため暗号処理の負荷が高くなり，最悪の場合書込み性能に影響を及ぼす。そのため生産性を落とすことなく暗号処理を実行するために，暗号化処理をハードウェア化する。

図 5 にハードウェア実装した AES コアのレジスタマップを示す。レジスタはコントロールレジスタと，4 つのデータレジスタで構成されている。1 つのレジスタは 32 ビット幅であり，ゆえに AES は 128 ビット版となる。表 1にコントロールレジスタの詳細を示す。まず初期化時に，コントロールレジスタの data set mode ビットを 1 にした状態でデータレジスタに鍵データをセットする。その後，data set mode ビットを 0 にしてデータレジスタに暗号/復号したいデータをセットする。暗号/復号に応じて mode ビットをセットし，start ビットに 1 を書込むことで処理が開始する。処理結果を取出す時は，start ビットを見ることで処理の状況が確認出来る。処理が終了したら，データレジスタに処理結果が格納される。

4.　機能検証

4. 1　暗号化性能評価　表 2に暗号・復号処理の実行環境を，表 3 に 1KByte のデータに対する暗号・復号化処理のソフトウェア実装とハードウェア実装の実行時間の比較を示す。ソフトウェア実装の場合，1KByte のデータを暗号化処理するために約 673.7ms かかっていたのに対し，

表 2. 暗合・復号化処理の実行環境

デバイス	Cyclone II
CPU	Nios II/f
周波数	100MHz
AES 鍵	128bit
処理の文字長	1KByte

表 3. 暗合・復号化処理の実行時間の比較

	暗号化	復号化
ソフトウェア実装	67372036 ticks (約 673.7 ms)	19273398 ticks (約 192.7ms)
ハードウェア実装	211773 ticks (約 2.1 ms)	69863 ticks (約 0.7 ms)

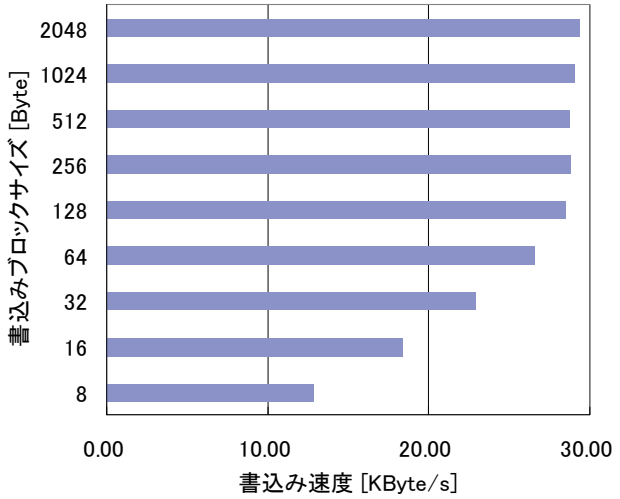

図 6. 各種ブロックサイズの書込み速度結果

ハードウェア実装をすることで約 2.1ms まで高速化することが出来た。この結果，例えば，64Byte の生産情報を暗号化する場合を例に考えると， 従来までのソフトウェア実装のときに必要な実行時間は 42ms となり，これ以上の生産性を得ることは不可能である。一方，ハードウェア実装した場合，64Byte のデータを暗号化するのに必要な時間は約 0.13ms となり，非常に高い生産性の生産設備にも対応することが出来ることが分かった。

4．2 書込み速度評価 書込み性能の評価を行うために，各種ブロックサイズ（8，16，32，64，128，256，512，1024，2048Byte）のデータを 800 回書込み，そのときの平均書込み速度を求めた。図 6 に書込み速度の結果を示す。グラフよりブロックサイズが大きくなるにつれ速度が速くなり，128Byte 以上のブロックサイズデータになると約 29KByte/s の性能が出ていることが分かる。これにより，例えば 64Byte のブロックデータを書き込む最大速度は約 26KByte/s であり，1 ブロック書き込むために必要な時間は約 2.35ms となる。これが本システムを用いたときの生産性の上限となる。

5. まとめ

本研究では，フィールド機器用ストレージユニットの開発を目指し，そのために必要となる項目について検討を行った。具体的には，①不正操作等によるデータ改ざん防止機能の実現手法，②大容量データの長期間安定記憶の実現手法，③盗難時のデータ読出し防止機能の実現手法，の 3 つについて検討を行った。①に関しては，データ保存媒体とユーザ空間を，RAM を用いて物理的に切り分けることで，物理的にアプリケーション側から書込みアドレスの直接参照をさせない仕組みを構築した。その結果，アプリケーション側からデータ保存媒体への不正アクセスを制限することが可能となった。②に関しては，フラッシュメモリの二重化によりハード的な信頼性を高めるとともに，WDT を用いてタスクの停止を検出・制御する機構を実現することでソフト的にも信頼性を向上させた。③に関しては，AES をハードウェア化することで実行速度を向上させ，書込み性能を妨げることなく暗号化を施すことが出来るようになった。

今後は実用化に向けて，具体的な対象にターゲットを当てた研究を行っていく予定である。

（平成 22 年 6 月 24 日受付，平成 22 年 8 月 26 日再受付）

文 献

(1) 21 CFR Part11, Electronic Records; Electronic Signatures— Scope and Application", FDA, http://www.fda.gov/RegulatoryInformation/Guidances/ucm125067.htm (2003)

(2)「薬食発第 0401022 号」, 厚生労働省 医療機器の承認申請等に係る関連通知, http://www.pmda.go.jp/operations/notice/2005/file/0401022.pdf (2005)

(3) ヒューレット・パッカード・カンパニー: 「カートリッジ・メモリ・システムを備えた WORM 磁気テープシステム」, 特開 2003－123342(2003)