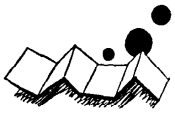
解　説



大規模製鉄所における情報処理システムの高信頼化技法†

斉藤　潔††　村山国弘††

1. はじめに

製鉄所の操業は，一部に設備の保守・更新等による休止がありうるが，24時間連続・年中無休止が通常である．一方，コンピュータによる生産管理業務の処理形態はオンライン・リアルタイム処理と数時間を最小処理サイクルとするバッチ処理の組合せである．したがってコンピュータによる情報処理システムも，操業システムの重要な一部として連続・無休止運転が原則となっている．

情報処理システムが，異常により停止した場合，製鉄所の生産活動全般に影響する．停止時間が数時間のオーダになると，経済的損失は数千万円以上となることが推定される．また大型・高温・高速等の特徴をもつ高炉・転炉・加熱炉・熱処理炉・圧延機等の諸設備と重量物である鉄鋼半製品・製品の物流設備の制御における安全確保および品質維持の面でも情報処理システムの信頼性はかかわりがある．

情報処理システムを構成している諸要素の信頼性はLSI等の素子レベルをはじめとし，装置レベルおよびそれらの組合せによるシステムレベルまで，年々高信頼化している．本稿では，そのようなシステムの構成要素をどのように組合せ，どのような運用方式を行って，情報処理システムレベルの高信頼化をはかっているかを中心に記述する．

2. 製鉄所の情報処理システムの特徴[1)]

2.1 コンピュータの利用形態

年産数100万トンから1,000万トンを越える大規模な銑鋼一貫製鉄所では **図-1** に示すように，管理センタに複数台の大型ビジネスコンピュータを設置し，オフラインコンピュータとオンラインコンピュータに分けて使用している．各工場現場にはオンラインコンピュータと接続されたプロセス・コントロール用ミニ・コンピュータと端末装置が設置されている．プロセスコンピュータには製造設備の制御系，センサ，マン・マシンインタフェース用端末装置が接続されている．

2.2 生産管理関係業務処理システムの概要

図-1 に示す本社コンピュータで需要家からの注文情報は設計品質等の諸情報を付加され生産指示として製鉄所のオフラインコンピュータへ送信される．この注文データ1件ごとの生産指示をもとに，オフラインコンピュータでは，工場ごとの生産計画を作成する．

この生産計画は数時間ないし日単位にオンラインコンピュータへ渡される．そこでさらに具体的な作業指示となり，工場内の各端末機，プロセスコンピュータへ必要なタイミングで渡される．その作業指示に従った生産現場での作業および設備の運転制御等の結果は，作業実績として刻々収集される．この作業実績は，当該工程の次の作業指示および前後する工程の作業指示・変更指示に反映される．またこの作業実績は集約されてオフラインコンピュータに渡され，次のサイクル以降の生産計画に反映されるとともに，管理者用の諸報告書および統計類が作成される．

3. 情報処理システムの信頼性の考え方

3.1 信頼度要求水準

製鉄所に限らず一般的に情報処理システム全体の信頼度はそれにかかわる諸要素の信頼度の総合として，**図-2** のようなモデルとして表現できる．

製鉄所のシステムは，ある程度独立的な主要工場* 対応のアプリケーションシステムの複数システムから構成されている．各システムごとに設計思想や工場の操業方法の違いにより要求信頼度は異なるが，異常による 図-2 の直列モデル全体の停止時間は，数時間から数分まで，また月間稼動率** として99.9%前後以

† Technique for High Reliable EDP Systems for Large Scale Steel Works by Kiyosi SAITO and Kunihiro MURAYAMA (Fujitsu Ltd.).

†† 富士通(株)第一製造工業システム部

* 厚板圧延工場，薄板熱間圧延工場，薄板冷間圧延工場等

** 月間稼動率 $=\frac{\text{月間総時間}-\text{月間計画的休止時間}-\text{月間の異常によるシステム停止時間}}{\text{月間総時間}-\text{月間計画的休止時間}}\times 100\%$

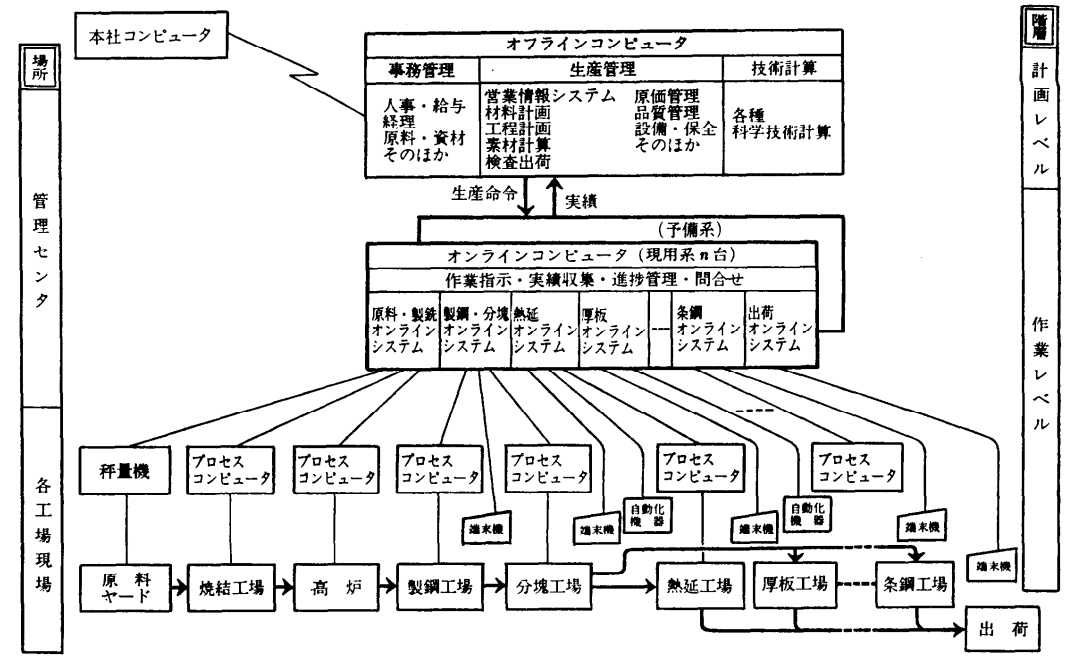


図-1　製鉄所コンピュータシステム概念図

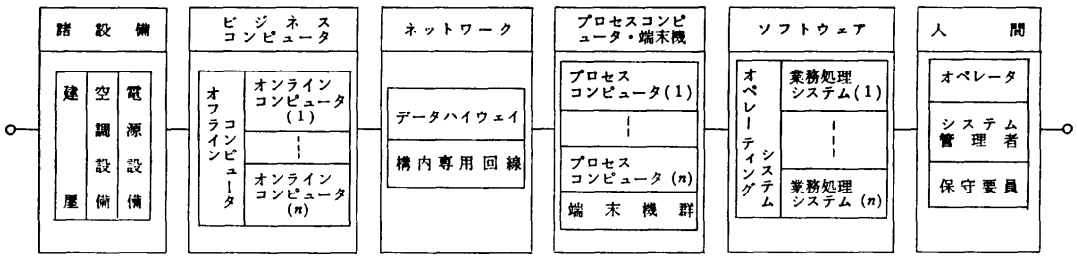


図-2　情報処理システムの信頼度モデル

上が一般的要求水準である．

システム停止時間の許容限度は，現場作業あるいはプロセスコンピュータでの制御をシステム停止以前に渡されている情報で続行できる時間，またはシステム停止とともに即時作業停止してもその停止時間をロスタイムとして許容できる時間をもとに設定される．この設定は，システム設計時点での重要な検討項目である．

3.2　高信頼化技法の適用についての考え方

信頼度の要求水準を達成するためにとられている手段をここではすべて高信頼化技法と呼ぶことにする．

製鉄所の情報処理システムには，設備や操業技術の改善等に対応してたえず変更がある．この変更作業のための停止時間についても短縮化の要求がある．これへの対応も含めた高信頼化技法の適用が必要となっている．高信頼化技法は，システム停止時間と停止頻度を許容水準以下に維持すること，および停止による生産活動への影響範囲を限定することを目的とする．これらは，コンピュータシステムの配置・機能分担方式，システム構成方式，復旧方式，運用・管理方式等に対して技術的・コスト的見地からバランス良く適用されねばならない．

このような考え方で次項のような高信頼化技法が適用されている．

4.　適用されている高信頼化技法の具体例[2)]

4.1　コンピュータシステムの配置・機能分担方式

図-1 で示したコンピュータの利用形態は次のよう

な高信頼化技法によって形成されている．

1) 管理センタのビジネスコンピュータは，信頼度要求水準の異なるバッチ処理主体のオフラインコンピュータとオンラインリアルタイム処理主体のオンラインコンピュータに分けられる．オンラインコンピュータはさらに複数台で構成する場合もある．

2) 事務処理の機械化の分野と製造設備の自動最適制御の分野に適合するコンピュータは異なるのでそれぞれの分野に対応して設置する．

3) プロセスコンピュータは製造設備単位に設置し，制御の範囲を限定する．

4) オフラインコンピュータ，オンラインコンピュータ，プロセスコンピュータの各レベル間および同一レベルでの機能分担範囲を相互の結合度・依存度がある程度「粗」となるように設計する．

以上により処理機能の維持，異常の影響範囲の限定，運用・管理の容易化をはかっている．

4.2 システム構成方式

ハードウェア関係の構成方式は同一装置の多重化構成が基本である．

（1） ビジネスコンピュータ

(イ) 本体装置：中央処理装置，チャネル制御装置，チャネル，主記憶装置等のうち必要なものを多重化する．多重化された装置のどれかに異常が発生しても，オペレーティング・システムの機能により，本体装置としては無停止でフォールバック運転へ移行できる確率が増す．

さらに，この本体装置と同一性能レベルの装置を設置し，予備機兼システム開発兼メンテナンス用とする．

(ロ) 外部記憶装置の制御装置：磁気ディスクやテープ装置の制御装置は複数台設置し，複数チャネルとともにアクセスパスを多重化し，異常時フェールセーフとする．

(ハ) 各種周辺装置：予備装置を含む冗長構成とする．磁気ディスク装置では，同じデータファイルを別別の装置に二重に配置しフェールセーフ化を行う場合もある．

(ニ) 切替装置：予備装置への切替えを手動で行う装置については遠隔切替装置を設置する．

（2） ネットワーク

製鉄所ではデータハイウェイ[3]および Point To Point あるいは Multi Drop の構内回線が用いられる．

データハイウェイの主要部は二重化され，現用・予備ループ切替え，バイパス・ループバック機能を持っている．

ネットワークでは，断線事故・外部ノイズに対してケーブルの選択および布設工法で高信頼化がはかられる．最近では光ファイバ・ケーブルを採用し外部ノイズ対策をとるケースが多くなっている．

（3） プロセスコンピュータ

ビジネスコンピュータと基本的には同じ考え方であるが，オンラインコンピュータ接続の端末機を併設し，プロセスコンピュータ異常時においては，その端末機からの入出力情報で手動制御を行う方式により多重化の程度を低くする場合がある．

（4） 端　末　機

一般事務所と比べて悪い環境に設置されるので，防塵・防蝕・耐震対策，絶縁・アース・漏洩電流など電気的環境への配慮および操作性への配慮のなされた装置を必要とする．

端末機は近辺に設置されたもの相互間でバックアップする方式（ソフトウェア機能で代行入出力を可能とする）と予備機によるバックアップ方式がある．

（5） 諸　設　備

(イ) 建屋：地震対策として建屋そのものおよびフリーアクセスの強化を行っている．コンピュータ機器自体にも倒壊防止対策をとる場合がある．

(ロ) 電源設備：コンピュータ機器・データハイウェイの中継器・端末機へ専用の安定化電源設備から供給する．その電源設備は多重化し，現用設備の異常時には無瞬断あるいは手動により予備機へ切替える．供給系統を分け影響範囲を限定する場合もある．

(ハ) 空調設備：複数設備により負荷分散・危険分散を行う．また予備設備を持つ．

(ニ) 警報器：コンピュータの運用状況（運用中，休止中，復旧処理中等）を端末設置場所に一斉に通知する警報システムを設置する場合もある．

4.3 復 旧 方 式

システム構成要素の異常発生時は，前項の構成方式により代替機でフォールバック運転を行うことが基本である．異常装置は適当な時点でシステムより切り離して修復を行い，再度適当な時点でシステムへ復帰させる．

コンピュータの異常発生時，処理機能がフェールセーフとならず停止した場合には，処理再開の前にデータファイルの復元を行わなければならない．データファイルは，一部でも失われた場合と突然の処理停

止またはソフトウェアの異常終了により論理的整合性がとれていない場合とがある.

前者の場合，データファイルの復元のためには，適当な時点・間隔で別な装置媒体にコピー・保存をしておく．さらにそのコピーを採取した時点からシステム停止直前までの状態に復元するために再処理用として入力データを保存するか，重ね書き用として更新後データの保存のいずれかが必要である.

後者の論理的整合性の復元のためには，復元時間をより短縮するため，更新前データを保存しこれを使って論理的整合性がとれている処理時点の状態にまで書き戻す方式がある．この場合数秒のオーダで復元できる.

これらの復元方式は最近のメーカ提供のオンラインデータベースシステム(例：FACOM AIM (Advanced Information Manager) では標準的にサポートされているが，ユーザレベルで実現しているシステムもある.

最近ではシステム停止の検知，調査資料の採取，切替え，再開始処理の一連の措置手順を半自動化できるハードウェア・ソフトウェアの機能が提供されている.

データファイル復元後の処理再開は，中断となった処理のためのデータの再入力またはそれが自動的に保存・処理された場合には，その直後のデータの入力から行われる.

4.4 運用・管理方式

以上の各方式における高信頼化技法を十分生かすため，オペレーション面，ハードウェアおよびソフトウェアの保守面においても簡易化・標準化・目標管理等の高信頼化技法を適用している.

(1) オペレーション

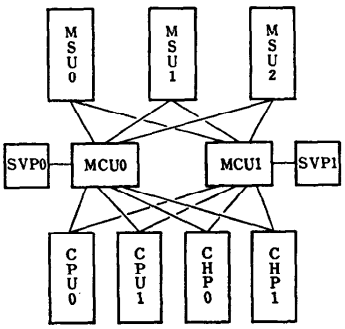
オンライン・リアルタイムシステムでは端末機での入出力操作を簡易化するために，会話的処理を基本に入力ガイダンスの表示，入力データチェックの徹底，処理途中での取消し・変更機能を適用している.

管理センタのコンピュータのオペレーションでは，相互関連のあるジョブの開始・終了を与えられたスケジュールで自動コントロールするようシステム化している.

システム停止時間を一定水準以下に保つため，異常時の措置手順を標準化している.

(2) ハードウェア保守

異常発生時，所定時間内に保守員が到着できる体制が 24 時間とられている．予防保守の見地から，オペレーティング・システムで採取されている異常状況ロギングデータをチェックし，異常があれば対処を準備し定期保守日等に措置をする．現用機の定期保守は予備機と切替えて行う．ただし，オフラインコンピュータは休日等に停止して行う場合もある.



MSU : Main Storage Unit
SVP : Service Processor
MCU : Memory Control Unit
CHP : Channel Processor
CPU : Central Processing Unit
(個別ChannelはCHPに含まれる．図では省略している.)

図-3 本体装置の構成例 (FACOM-M-200)

異常装置は早期修復が原則であるが，修復のためにシステム停止を伴う場合は，工場操業に影響の少ない時間帯に行う.

コンピュータ関係の機器の増設・変更作業は，その所要時間が数時間以上の場合，工場の生産計画レベルの調整を行い実施する場合もある.

所定時間内に増設・変更作業が終了しない場合，旧システム状態に戻して運転ができるような工事方法とし，数時間のオーダで数回に分けて段階的に行う場合もある.

(3) ソフトウェア保守

ソフトウェア保守はオンラインデータベースシステムを含むオペレーティングシステムと業務処理システムのプログラム・各種定義情報を修正・変更・追加を行うことである.

これらは予備機で事前確認テストを行ってから現用機へ適用している．現用機でも再度テストを行ってから実運用に入る．適用タイミングはハードウェア保守と同じにする場合が多い.

(4) 管 理

顧客およびメーカの関連スタッフによる総合的な運営体制のもとで，ハードウェア・ソフトウェアの障害管理が行われる.

異常状態は大小を問わず発見者から所定の書式で管

理担当者へ報告され，登録後，各担当者へ振り分けられる．各担当者は適切な措置を行いその内容を記入して管理担当者へ返却する．

異常内容・件数・措置状況・システム稼動率を定期的にまとめ運営会議で評価・解析する．これらは目標管理の対象とし，目標を達成していない場合は，対策を検討し重点的に実施する．

標準化された手順以外の保守作業は計画書を作成しチェック・承認を受けて実施され，かつ実施後の評価報告が義務づけられる．

5. むすび

コンピュータ等のハードウェア個別の信頼度およびオペレーティング・システムの機能は向上しているが顧客レベルでは最終的に情報処理システム全体の無停止運転を望んでいる．ハードウェアのコストパフォーマンスの向上により，特に磁気ディスク装置・媒体の異常時のデータファイルのフェールセーフ化や本体装置の予備機切替え時の停止時間の極小化等がメーカレベルで実現・提供されることが期待されている．

さらに，ハードウェア・ソフトウェアの保守がシステム運転中に容易に行える機能が期待されている．

本稿は主として筆者の製鉄所システムにおけるシステムエンジニアとしての作業経験をもとにまとめた．

顧客各位のご指導に感謝する．

参考文献

1) 鉄鋼年鑑，pp. 591-600 (昭55)．
2) 斉藤他：鉄鋼生産ラインにおけるオンラインシステムの信頼性対策，FUJITSU, Vol. 29, No. 6, pp. 261-279 (1978)．
3) 八星，鈴木，三田，山口：データハイウェイシステムの動向，情報処理，Vol. 21, No. 8. pp. 872-879 (1980)．

(昭和56年12月7日受付)