3.32 周期起動を持つシステムに関する教訓（T32）

教訓 T32

周期処理、「時間」と「変化」を監視せよ！

問題

A 社の物流センターの制御システムは、同期して連係動作する多数の PLC（Programmable Logic Controller）[14] により構成され、新型 PLC と旧型 PLC が混在していた。

ある日の早朝、A 社工場内の制御ネットワークで障害が発生した。

ネットワーク復旧後、運転再開のため、「再稼働初期設定」機能を実施した（図 3.32－1 ①）。「再稼働初期設定」機能とは、監視制御サーバから各 PLC の制御装置に対して、その保持する最終稼働状況（稼働が仕掛状態となっていた個所）の検索を行い、その中断個所を初期化し、各制御装置の開始時点の同期を合わせる機能である。この機能を実施したところ、旧型の PLC の制御装置が正常に作動せず、ハングアップ状態となり（図 3.32－1 ②）、その原因究明と対処のために制御システムの復旧が大幅に遅れた。

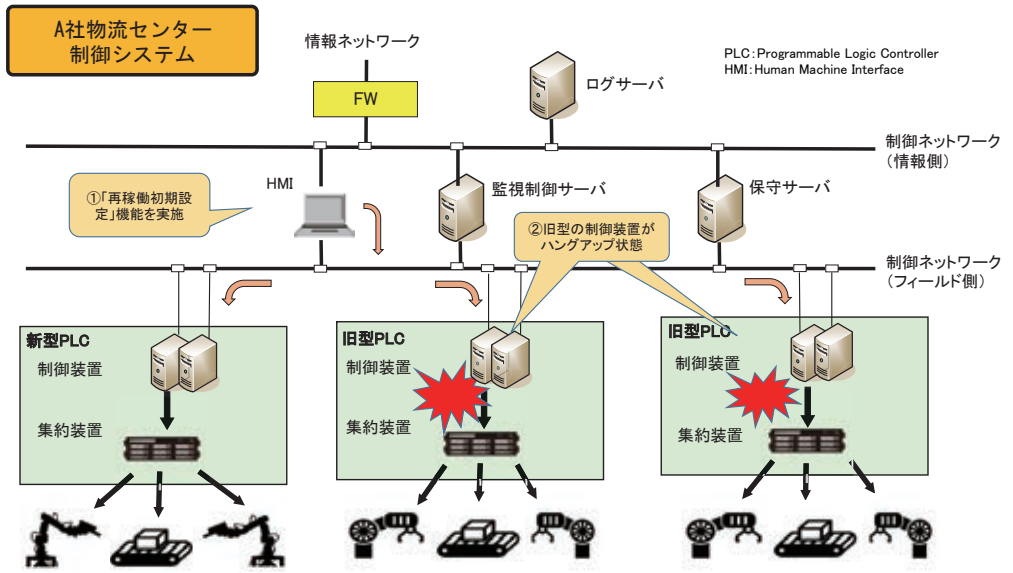

図 3.32－1　障害状況

[14] リレー回路の代替装置として開発された制御装置。自動機械の制御に使われる。

原因

A 社の制御装置のソフトウェアは、制御ネットワークからコマンドや制御情報をイベント発生時に受信・登録する処理「イベント処理」と、周期起動でコマンドや制御情報を受け取り、集約装置を稼働させたり、制御情報を更新させたりする処理「周期処理」の 2 つで構成されている（図 3.32－2）。監視制御サーバから発せられた「再稼働初期設定」コマンドは、イベント処理により登録され、周期処理により取り出されて実行される。

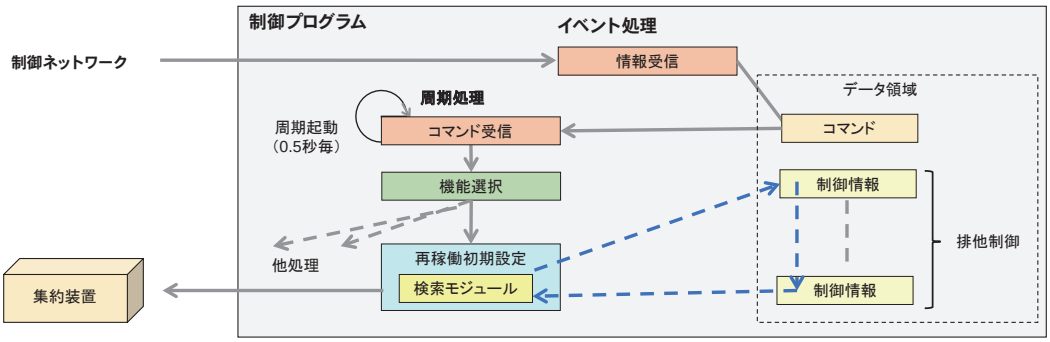

図 3.32－2　制御装置　ソフトウェア構造

制御システムの復旧が大幅に遅れた直接原因は、今回の「再稼働初期設定」機能の実施によって、旧型（20 年以上稼働）の PLC の制御装置上での周期起動で開始する「コマンド受信」から「再稼働初期設定」の検索までの処理が、周期時間内（1 サイクル当り 0.5 秒）で処理が完了しなかったため、以降の周期処理のコマンドが次々と滞留し、その制御装置に高負荷状態が発生し、ハングアップ（無応答）状態となったことであった。

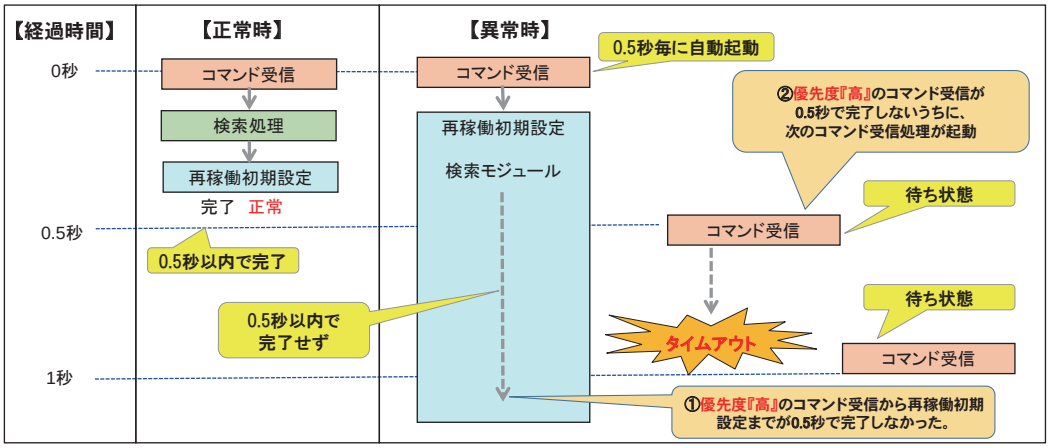

図 3.32－3　障害原因

監視センターから実行した「再稼働初期設定」機能が、各制御装置に命令を出した。旧型 PLC の制御装置は、「コマンド受信」から「再稼働初期設定」を実行した。それは、本来 0.5 秒以内で行える処理であったが、今回は、「作業開始時点から現時刻（昼過ぎ）までの、対象となる制御情報」を検索する際に制御情報が想定数以上存在したため、0.5 秒以内で完了することができなかった（図 3.32－3 ①）。そのため、0.5 秒ごとに「コマンド受信処理」が起動され、これらが連鎖的に遅れたため、旧型 PLC の制御装置は、ハングアップ状態となった（図 3.32－3 ②）。

周期処理は、ひとつの完結する処理群が周期時間内に完了することが条件であり、新たな機能や、制御すべき機器が増えた場合でも、その周期内で処理が完了することは必須である。すべてのコマンド処理が正常に稼働するかを事前に実機で確認すべきであった。

「再稼働初期設定」機能は制御システム導入時に作られたものだが、障害時にだけ使う機能であったため、長年このコマンドを実行していなかった。その間、集約装置につながれた機器の増加や、流れる制御データの増大、ネットワークの長時間の停止による検索処理時間の増大を考慮する、などの実行環境の変化に気づかなかったにも関わらず、障害マニュアルでは、使われるツールとして記載されていた。

したがって、根本原因は、周期処理を持つ制御システムについて、その周期時間を管理しておらず、新しい環境の変化があった場合の周期時間の見直しや、すべての PLC 機器について動作確認を行っていなかったことである。

また、A 社の物流センターの制御システムで使用している PLC は、コンピュータ部分のようなライフサイクルが比較的短い制御装置と、メカ部分のようなライフサイクルが非常に長い集約装置が一体となっている機器であった。そのため、機器全体の交換時期が設定しづらい装置であった。今回のような集約装置につながる現場機器の増設が行われ、また検索に時間がかかるような制御装置の処理速度上の問題がリスクとして潜在化し、最新の制御装置に交換しなくてはならない事態になっても、コスト面の関係からすべての PLC を旧型から新型に入れ替えることがなかなかできない状態であったことも根本原因の一つとしてあげられる。

対策

周期処理が含まれる制御システムの機能追加を確実に実施する対策として、以下の 3 点を実施することにした。

⑴ 周期時間管理

周期処理が組み込まれている制御プログラムで設定されている周期時間を管理するとともに、その周期時間を超える場合がないかを適宜監視する管理ルールを定める。このような周期時間管理は、制限値管理と同様な管理方法となる。

さらに、周期処理の周期時間を超え得ることを考慮したプログラムロジックも検討することとした。

（例）立ち上がった周期処理は、前の周期処理が完了していない状態で、かつ 0.5 秒を経過した場合、実際の処理を行わずに終了し、結果を監視に通知（または監視が検知）する仕組みとする。

⑵ 新機能追加時の運用ルールの策定

- 機種ごとの仕様をもとに周期時間を評価した上で、すべての機種について動作確認を実施する。
- 障害対策を設計時に検討し、マニュアルに追加する。そして、検証時は、どこまでの検証を行うか、関係者と議論し、「テスト一覧」を作成する。それをもとに、できない検証についてのリスク評価を行い、その対策の手順を明確にし、対策マニュアルとして作成する。

以上、周期処理を持つ制御システムの機能追加の手順をまとめると、図 3.32－4 のようになる。

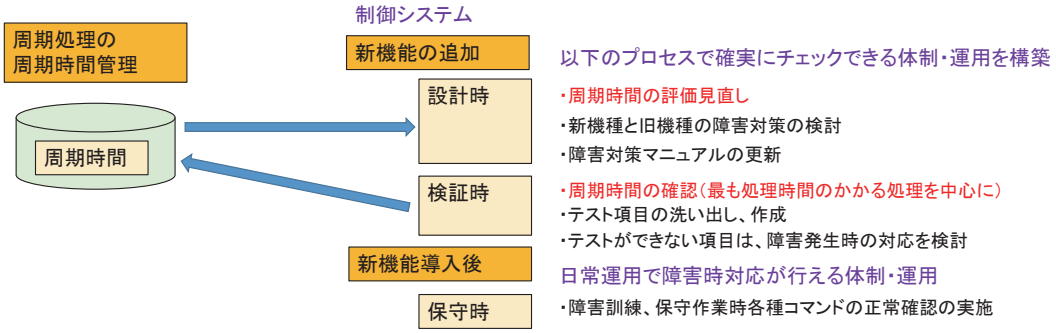

図 3.32－4　周期時間管理と制御システムの機能追加との関係

⑶「旧機種の装置を新機種の装置に更新しやすい」構成を作る

今回の場合、遅い PLC の制御装置を最新の高速な PLC の制御装置に置き換える対策もある。しかし、A 社の PLC は、制御装置と集約装置とが一体となっているため、製品寿命の短い制御装置だけではなく PLC 全体を入れ替えなくてはならず、高コストとなっていた。

近年、この制御装置と集約装置の内部 I/F（インターフェース）が、独自プロトコルでなく、汎用的なイーサネット（Ethernet）になった。

そこで、制御装置だけを入れ替えられるように、両装置間の I/F がイーサネットで、制御装置 - 集約装置分離型の PLC をベンダに製造してもらうことを要請した。この分離型の PLC を導入することで、ベンダの制約が緩和されるとともに、新制御装置だけの入替えもできるようになった（図 3.32－5）。

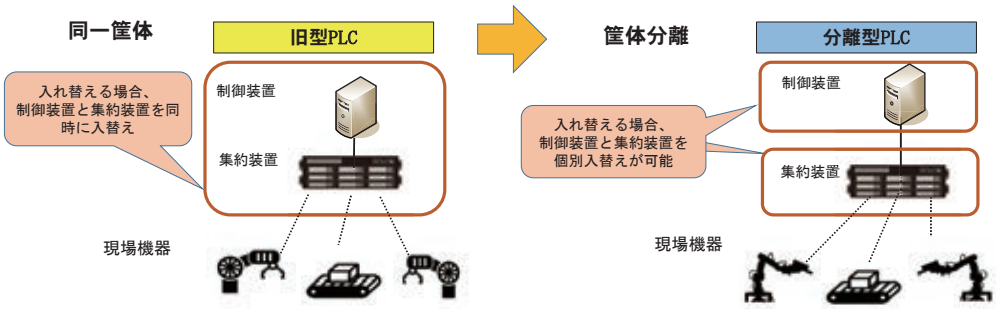

図 3.32－5　分離型 PLC

効果

制御システムの周期時間は、設計時にすべての処理時間を考慮して決定される。当然、周期時間が短ければ処理効率がよくなるが、短すぎると今回のような障害を引き起こしたり、空振りや CPU 負荷増となったりする。そのようなバランスの上で決定された周期時間は、制御対象機器が増えたり、制御データが増大したり、新規機能追加や新型機器が導入されたりすることにより、見直す必要性が生ずる。この教訓は、制限値管理の「制限値」と同様に、「周期時間」の変化を見逃さない周期時間管理の重要性を気づかせてくれる。

制御システムの周期処理に新旧の制御装置が混在する場合は、性能差が生ずることから、システム全体の構成に注意が必要である。その際には、製品の入れ替えを容易にする製品構成についても検討する機会を持つことができる。

教訓

一般的に、制御システムは、20 年以上使うこともよくあり、使用中に部品の供給が中止になったり、ソフトウェアやハードウェアの保守契約が切れたりすることが多い。そのような状況において、コストの面から一度にシステム内のすべての装置を更新できないことから、同一システムの中に、徐々に新型の高性能な機器が導入され、新旧の機器間で処理時間に違いが生ずることが多々起こる。また、長期の間に運用方法も変わり、今まで使われてこなかった機能が使われるようなことも起こる。その中で、周期時間は、制限値と同様に変化を見逃さない管理方法が必要である。具体的には【教訓 T4】で述べている変化点管理を対策とすることができる。

【教訓 T4】システムに影響する変化点を明確にし、その管理ルールを策定せよ！

制御システムは、比較的短期のうちに性能が上がっていくコンピュータ部分と、長期にわたって使用していくメカニック部分が混在する機器がある。このような状況も踏まえ、短期間で交代可能なコンピュータ部分と長期間使用するメカニカル部分を分けた機器構成も検討する必要がある。

この教訓は、そのような制御システムに対する運用管理とシステム構成の在り方を教えてくれる。