長期的な制御システム保全計画による火力発電プラント安定稼働実現へ：DIASYS Netmation の最新ソリューション

Maintaining Operational Availability through Long-Term Maintenance Planning of Control System: The Latest Solutions of DIASYS Netmation

三菱重工業株式会社
エナジードメイン
GTCC 事業部 サービス技術部

火力発電プラントが，旺盛な電力需要に応え，安定稼働するとともに，中長期にわたる持続可能な運用をするためには，本体設備のみならず，監視・制御を司る制御システムの保全活動が極めて重要であり，制御システムの保全活動は設備運用に極力支障を与えぬよう計画されることが求められている。制御システムの保全には，安定稼働のための定期交換・更新作業や，電子部品に対する生産中止対応があり，本体設備側の点検停止期間中に保全活動ができるように，制御装置の入出力通信部分のみを効率的に更新することを可能とする FXtoLS アダプタを開発した。また，IoT 技術の発展に伴い，稼働中の制御システムに対するサイバー攻撃のリスクが増大しており，多層防御に基づくサイバーセキュリティ対策を DIASYS Netmation の最新ソリューションとして紹介する。

1. はじめに

再生可能エネルギーの導入が進む中，AI 等による膨大な計算量を支えるためにデータセンターの電力消費量が急増する等，今後も世界中で旺盛な電力需要が見込まれている。安定した電力供給を維持するためには，依然として大規模かつ高効率に電力を生むことができるガスタービンに代表される火力発電は欠かせない存在であり，急激な需要の変動や，天候に左右される再生可能エネルギーの発電量を補完する役割としても重要な役割を担っている。その中で，火力発電プラントの安全かつ安定運用を支えているのが制御システムである。制御システムは，発電プロセスの制御，監視，最適化を行うプラントの運用基盤であり，加えて，遠隔監視システムや異常予兆検知など，クラウド基盤技術を活用・連携することで，プラントの最適運転や運転支援といったお客様の運用ニーズに応えてきた。したがって，計画的な制御システムの保全や更新は，火力発電プラントの持続可能な運用の鍵であり，プラントの安定稼働の実現のために，プラントの長期的な運転計画と合わせて制御システムの保全計画を行なうことが重要となる。本報では，三菱重工業株式会社（以下，当社）が製造する制御システムである DIASYS Netmation の最新ソリューションについて紹介する。

2. 制御システムのライフサイクル

制御システムは，図 1 に示すとおり，プラントの制御演算や各計器とのプロセス信号の送受信を行なう『制御装置』と，監視員やエンジニアが操作する『操作保守計算機』の大きく 2 つに分けられる。

制御装置はコンデンサや半導体などの電子部品で構成されており，素子や部品レベルでの EOL（End of Life）や後継品の提供体制を含めたライフサイクルは 10～15 年程度である。

操作保守計算機は一部を除き Microsoft 社の Windows OS を搭載した計算機であり，計算機

自体のライフサイクルは一般的に 5 年程度と言われている。また，Windows OS も近年，セキュリティ対応強化等により世代交代のサイクルが短くなっており，Microsoft 社による最新の業務用 OS ライセンスのサポート期限は 5 年間が一般的である。(組込み機器向け OS ライセンスの場合は 10 年間)

火力発電プラントの寿命を 30 年程度と仮定すると，プラント運用の中で制御装置は 1～2 回，操作保守計算機は 3～5 回程度の更新が必要となる。従い，当社は製造メーカとして，発電事業者が予め長期的な制御システムの保全計画を立てられるよう，後述するソリューション提案を通じてお客様の事業運営の支援を行なっている。

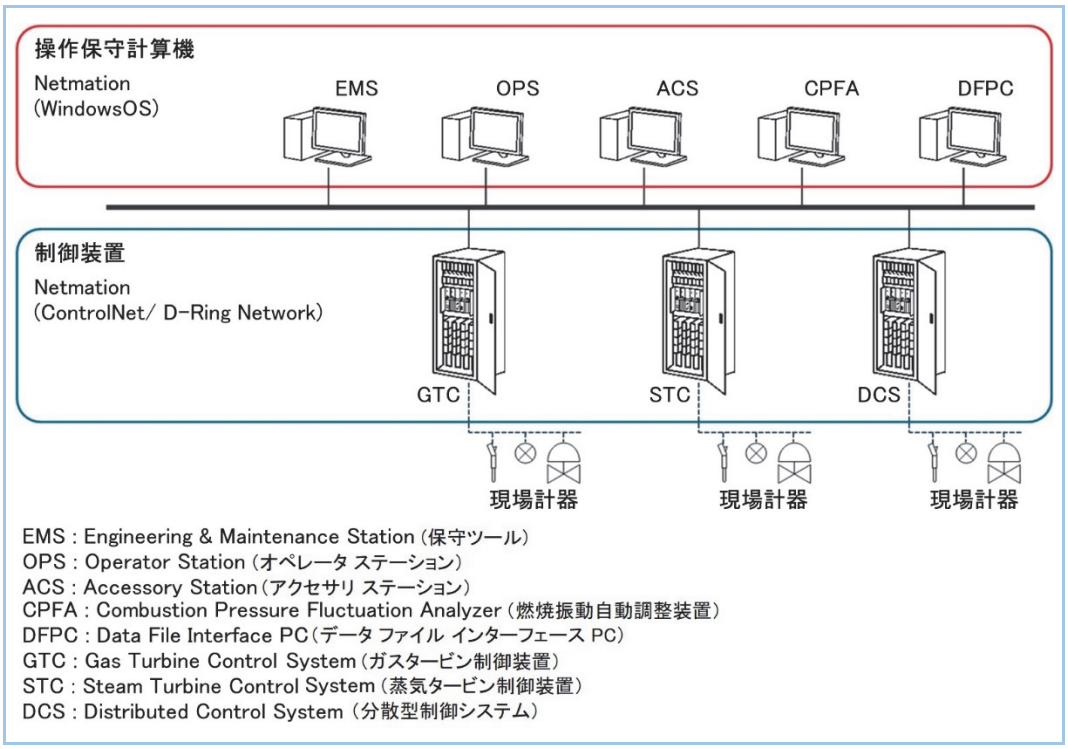

図1　制御システムのシステム構成

3. 制御システム保全のソリューション

本章では，DIASYS Netmation の維持・更新といった保全に関するソリューションを紹介する。

3.1　部品の定期交換

プラント設備が停止する定期検査などのタイミングで部品を定期的に交換することで，予防保全として経年劣化による機器の故障によるプラント運転への影響を未然に防ぐことが可能となる。

そのため，当社では制御システムで使用されている部品について，定期的な交換を推奨している。主な部品の推奨交換周期は図 2 のとおりである。

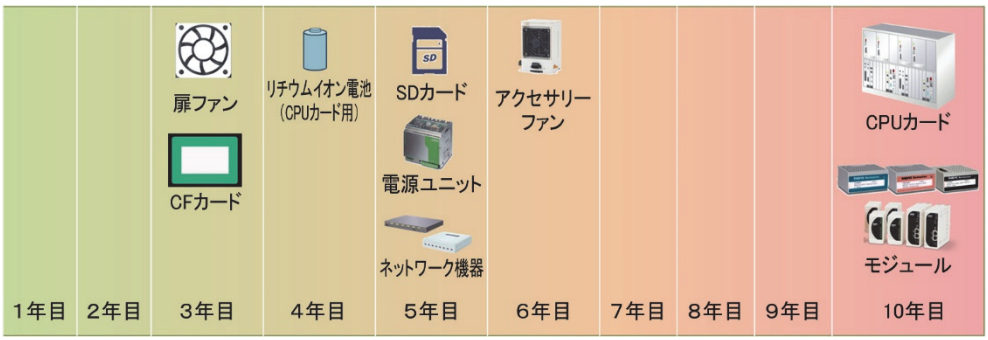

図2　主な制御システム部品の推奨交換周期

3.2 I/O ネットワーク更新

制御装置は制御演算などを行なう CPU や，操作保守計算機と通信を行なう通信カードなどで構成される『コントローラ部』と，現場側の各計器とのプロセス信号の送受信を行なう I/O モジュールや I/O モジュールとの信号を CPU と通信するアダプタなどで構成される『I/O ネットワーク部』に大きく分けることができる。

コントローラ部は，構成する電子部品の生産終了による型式変更があるが，上位互換を保ちながら後継機をリリースしており，定期交換や後述する I/O ネットワーク更新，操作保守計算機更新のタイミングで最新型式に更新することを推奨している。

I/O ネットワーク部については，DIASYS Netmation の I/O ネットワークは 2000 年にリリースされた『ControlNet』と 2014 年にリリースされ，現在新設発電プラントでも採用されている『D-Ring Network』があり，老朽化した I/O モジュールやアダプタを最新化するため，当社では，図 3 に示すように，I/O ネットワークを ControlNet から D-Ring に更新する『I/O ネットワーク更新』を推奨している。

I/O ネットワーク更新では，制御装置の筐体ごと更新する手法の他に，設置場所の制約や極力手を加える範囲を減らす目的で，制御盤は流用して現地で I/O ネットワーク部分のみを改造する手法があり，当社では既設の設置場所や制御盤内のレイアウトなどを考慮して制御装置毎に最適な手法を提案している。当社では I/O ネットワーク部分のみを現地で効率よく改造するために，外部ケーブルが接続されている既設のモジュール端子台に D-Ring Network の I/O モジュールを取り付けるための変換アダプタ：FXtoLS アダプタを開発した（図 4）。このアダプタを用いることにより，I/O モジュールに接続されている現場計器からの外部ケーブルの解線範囲を減らすことで，現地での改造作業や改造後の検証作業を簡略化することができ，更新工事期間を短縮することが可能である。

なお，I/O ネットワーク更新に合わせて制御装置における CPU 部の構成部品（CPU カードや CPU 電源）の更新も合わせて実施することが，CPU 部の老朽化対策として有効である。

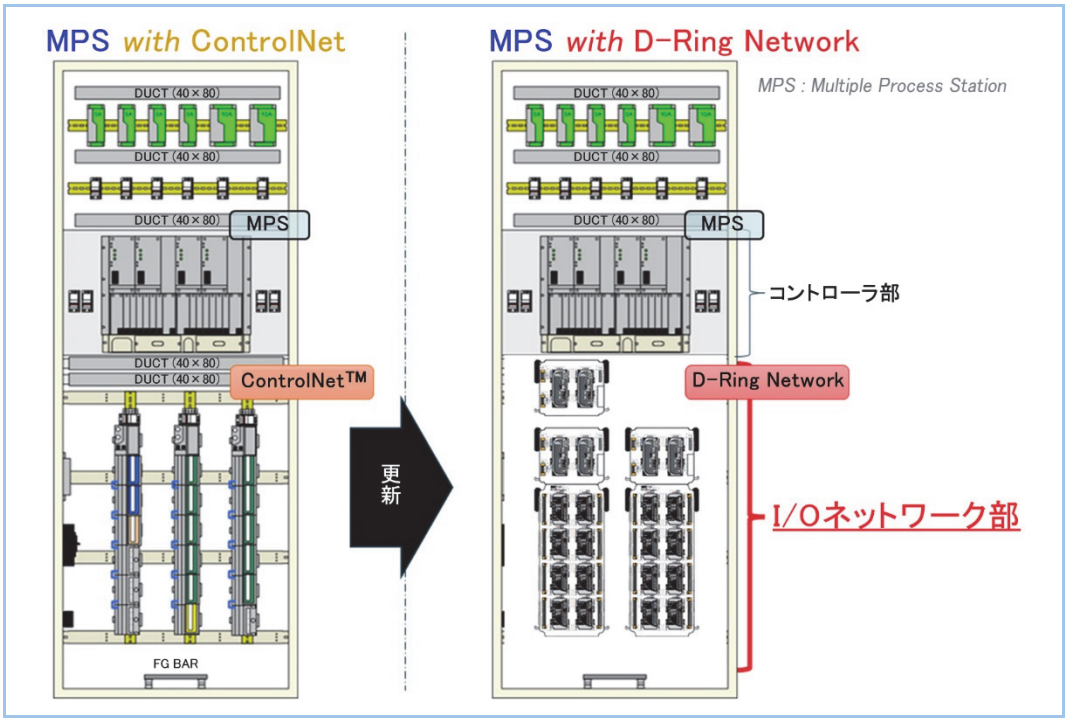

図3 I/O ネットワーク更新

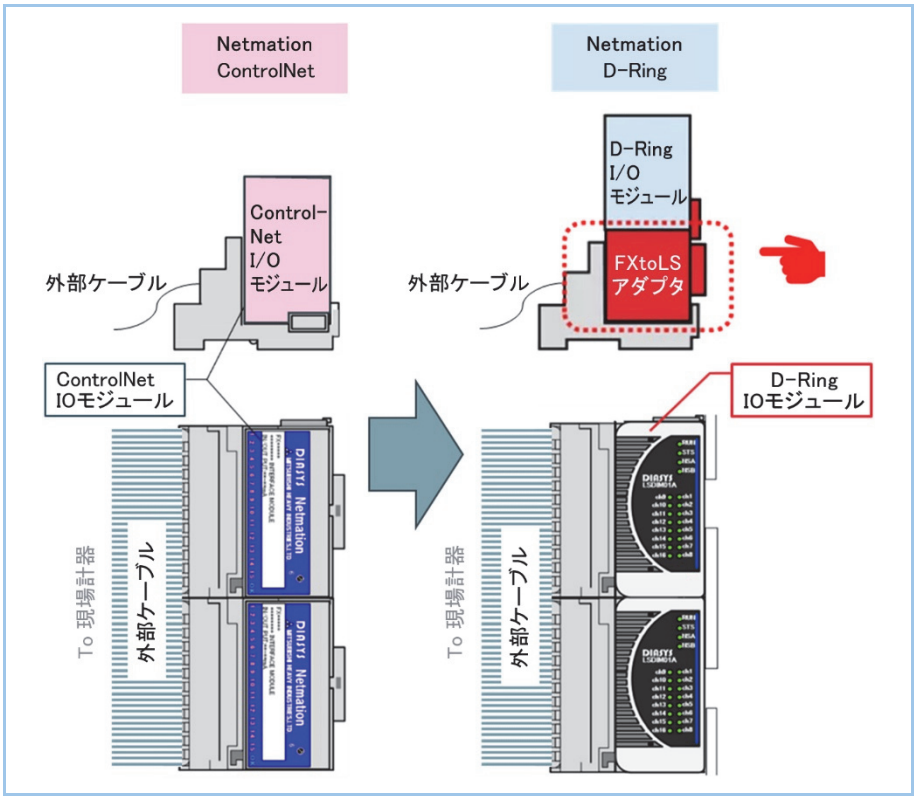

図4 FXtoLS アダプタ

3.3 STEP 更新

3.2 節で紹介した I/O ネットワーク更新は制御装置単位で実施することが可能である。具体的には，図 5 のように制御システムは複数の制御装置で構成されているケースがあり，定期点検など，プラントが長期間停止するタイミングに合わせて段階的に制御装置の更新を実施することが可能で，複数年度の各定期点検の期間に分散して，計画的に更新を進めることができる。

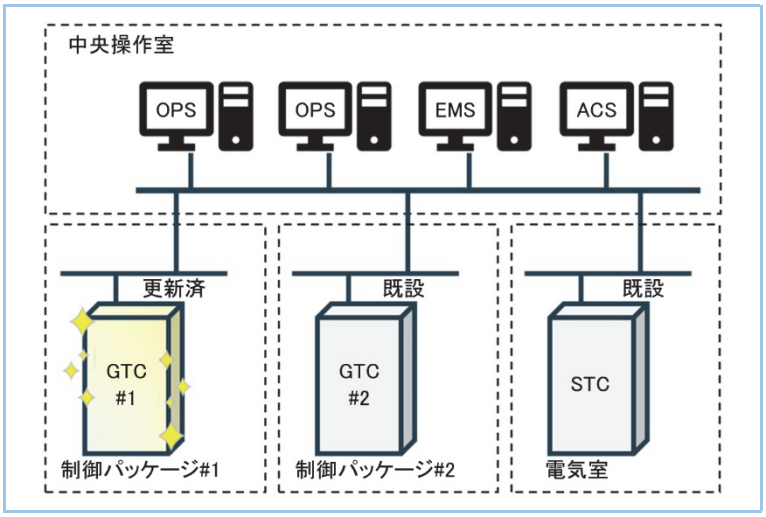

図5 STEP 更新のイメージ

3.4 操作保守計算機更新

ここまで制御装置の更新について紹介してきたが，本節では操作保守計算機更新について紹介する。操作保守計算機は汎用品の計算機を使用しているため，経年劣化により動作速度の低下やフリーズといったトラブルが増加する傾向がある。また，操作保守計算機は前述の通り Microsoft 社の Windows OS をベースとしているため，計算機で使用しているハードウェアの世代交代により古い Windows OS をサポートしている計算機は製造終了となり，予備品や故障時の代替品の入手が困難となる。計算機の世代交代の周期は年々短くなっており，計算機のライフサイ

クルは以前より短くなっていると言える。

また，前述のとおり Microsoft のサポート期間は 5 年程度であり，サポートが終了した場合は Microsoft から脆弱性修正のためのセキュリティパッチが提供されないため，セキュリティ的な観点からも，定期的な操作保守計算機更新の必要性は高い。

加えて，I/O ネットワーク更新においては D-Ring Network に対応した DIASYS Netmation のソフトウェアが必要となるため，当社では I/O ネットワークと並んで操作保守計算機の更新を計画的に行うことを推奨している。

4. サイバーセキュリティ対策強化

ここまで制御システムを健全な状態に維持するための保全のソリューションを紹介してきたが，本章では，近年需要が高まっているサイバーセキュリティ対策強化について紹介する。

近年，IoT 技術の発展と合わせてサイバー攻撃の脅威も高まっており，社会の重要インフラとして，プラントにおいても標的とされるリスクがあり，セキュリティ対策がより重要となっている。

国やプラントによっては，インフラ設備に対してサイバーセキュリティ対策を施すことを要求しているケースもあり，この流れは近い将来世界中に広がることが予想される。

当社では DIASYS Netmation のサイバーセキュリティ対策を強化するためのソリューションとして Netmation Protect Pack（以下，NPP）をリリースしている。NPP は図 6 のイメージ図のとおり，複数のサイバーセキュリティ対策の機能を持った多層防御によりサイバーセキュリティのリスクを低減するソリューションである。

制御システム構成図のうち，NPP がサポートしている機器・ネットワーク（カバー範囲）を図 7 に示す。NPP は制御システムのネットワークを介して接続される。なお，NPP の導入に際しては Microsoft 社のサポートを有した Windows OS である必要があるため，操作保守計算機は，Windows10 以降の OS に更新されている必要がある。また，常に有効なサイバーセキュリティ対策を維持するためには，NPP の継続的なメンテナンスや NPP を構成するソフトのライセンス更新が重要である。

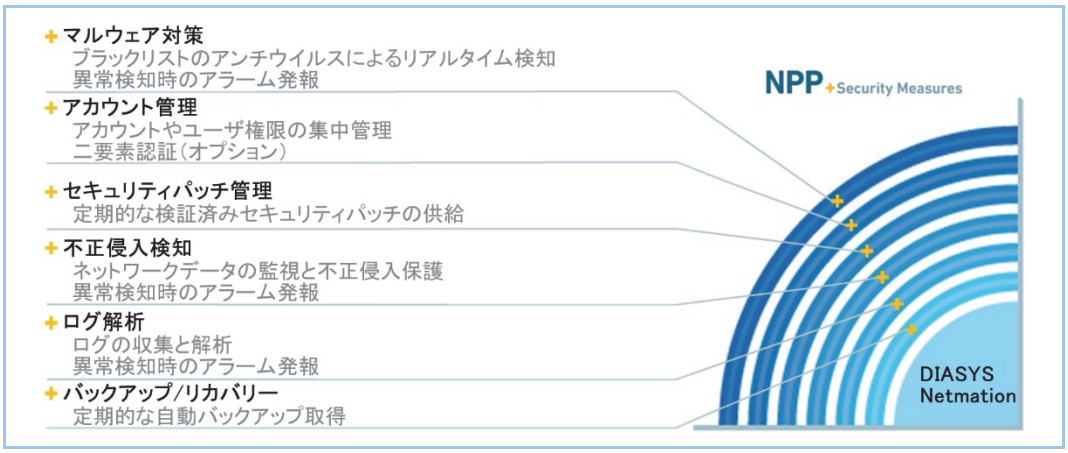

図6 NPP の多層防御

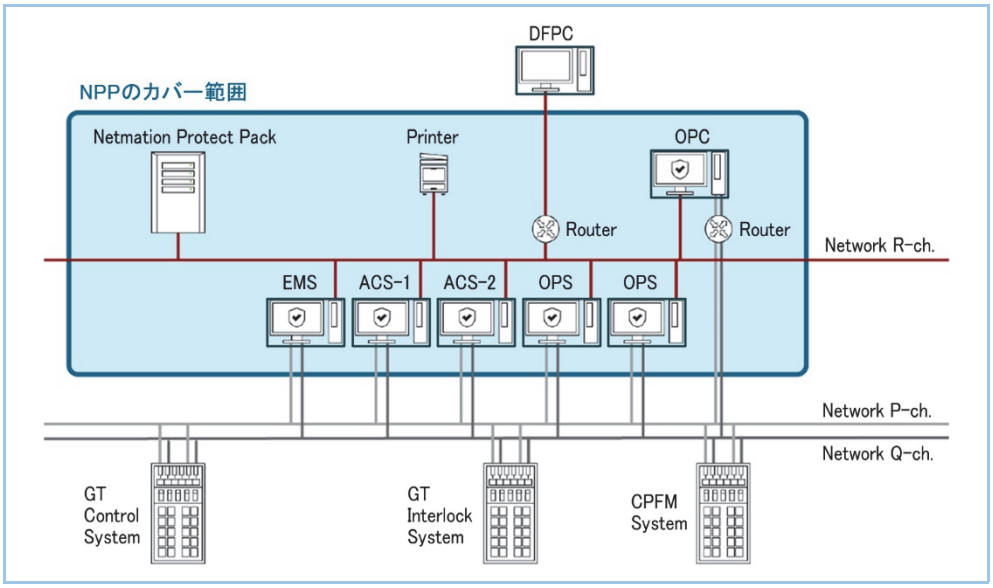

図7　制御システムにおける NPP のカバー範囲

5. 今後の展開

火力発電プラントの安定稼働を実現するためには，制御システムの維持・更新といった保全が不可欠である。当社は制御システムのライフサイクルに応じた適切なソリューションを提供し，プラントの長期的な運転計画と連携した保全計画の実現を支援する。これにより，予防保全や効率的な更新を通じて，プラントの運用を安全かつ安定的に維持することが可能となる。

長期的な視点を持ち，計画的な制御システムの保全を行うことは，プラントの持続可能な運用の鍵である。当社は，お客様のニーズに応じた最適なソリューションを提供し，プラントの安定稼働を支えるパートナーとして貢献していく。