デジタル計装制御技術

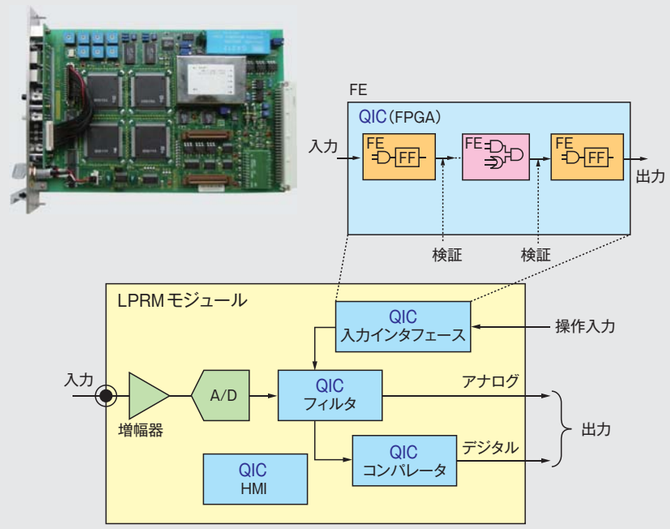
許認可動向を踏まえたデジタル安全系の開発と進展

原子力発電プラントの計装制御系は，安全な運転と管理を行ううえで極めて重要であり，最近では，最新のマイクロエレクトロニクス技術を用いたデジタル計装制御系の採用が進められています。デジタル計装制御系は，古典的なアナログシステムに比べて，経年劣化が少ない，機能変更や保守が容易などの特長がありますが，システムの動作がソフトウェアによって制御されるという特質のため，安全系を中心として新しい規制や指針が提唱されています。

東芝は，これらの規制・許認可動向に対応する世界市場に向けたデジタル安全系の開発を推進しています。

図1．第一世代デジタル安全系の外観 — 東芝初のデジタル安全系で，マイクロプロセッサを用い，高信頼性システムとして実現しています。

図2．第二世代デジタル安全系（デジタルトリップモジュール） — このモジュールは，FPGAを用いた第二世代デジタル安全系を構成するモジュールの一つで，対象とするプロセスパラメータが所定の値を超えたか否かを判定します。



FE：Functional Element　LPRM：局所出力モニタ　HMI：ヒューマンマシンインタフェース
FF：フリップフロップ　A/D　：アナログ／デジタル変換器

図3．第二世代デジタル安全系の検証方式 — ロジックをモジュール化し，QICを組み合わせて試験することで，システムの健全性を確保，確認します。

計装制御技術の特徴

原子力発電プラントの計装制御系は，万一異常が発生した場合に原子炉の安全を担う安全系と，その他の常用系に大別されます。安全系には，その特質から，常用系の異常が安全系に影響を及ぼさないように常用系と物理的かつ電気的に分離すること，相互に独立した多重化構成として単一の故障による全体機能の喪失を防止することなど，信頼性と安全性に関する厳しい規制が適用されます。

第一世代デジタル安全系

安全系は，当初，リレーやアナログ回路などハードワイヤード技術を用いていましたが，1980年代に，マイクロプロセッサを用いたデジタル安全系が提唱されました。これに対応して，ソフトウェアが正しく開発され実装されて，システムが健全に機能することを実証するシステムの検証と健全性確認（V&V：Verification and Validation）について，1982年のIEEE Std 7-4.3.2（電気電子技術者協会規格 7-4.3.2）及び1986年のIEC 60880（国際電気標準会議規格 60880，当時はIEC 880）など，標準や指針があいついで発行されています。わが国でも，1989年に日本電気協会から関連する初の指針としてJEAG4609初版が発行されています。

東芝は，これらの指針に合致する第一世代のデジタル安全系（**図1**）をいち早く開発し，1996年に運転を開始した東京電力(株) 柏崎刈羽原子力発電所6号機の安全系に適用しました。このデジタル安全系では，当社が保有している，ソースプログラムを書かずにロジック図を用いてソフトウェアを開発することができる技術を活用し，ロジックのすべてのパスを確認できるV&V手法を開発し適用しました。また第一世代デジタル安全系は，必要に応じてハードワイヤード回路も採用し，次章で述べるシステムの多様性に関する議論を先取りして考慮した設計としています。

第一世代デジタル安全系は，中部電力(株) 浜岡原子力発電所5号機にも適用し，良好な運転実績を示しています。

第二世代デジタル安全系

1990年代後半から2000年代初めにかけて，諸外国の規制当局及び関連機関の間では，それらの国々のデジタル安全系がまだソフトウェアをプログラムとして書き下す開発手法を主流としていたこともあり，デジタル安全系の共通因子故障（Common Cause Failure）への対応に対する議論が深まりました。

共通因子故障とは，同一の要因により，多重化されている安全系が機能停止に至る可能性のある故障を言います。共通因子故障への対応に関する議論は，米国原子力規制委員会（NRC）の図書であるSECY 93-087，NRCの審査ガイドであるNUREG-0800，前述のIEEE Std 7-4.3.2及びIEC 60880の改訂版などに反映されています。

これらは，共通因子故障に対する一つの対応策として，システムの多様性について言及しています。多様性とは，システムを異なる手法や形態で実現することを言い，前述のガイドや指針では，共通因子故障の発生を抑えることができると示唆しています。

この規制動向を受けて，当社は第一世代デジタル安全系とは実現形態や開発手法をまったく異にする第二世代デジタル安全系（**図2**）を開発しました。

第二世代デジタル安全系は，動作自体にはソフトウェアを必要としないFPGA（Field Programmable Gate Array）を用いて実現しています。第二世代デジタル安全系では，動作すべきロジックをFPGA内部にデジタル回路として埋め込み，この回路動作によりシステムを制御します。FPGAの内部にはソフトウェアは存在しません。第二世代デジタル安全系のV&V手法についても，**図3**に示すように，100％のロジックの検証が可能な範囲でロジックをモジュール化し，検証したモジュール（QIC：Qualified IC）を組み合わせて試験することで，システムの健全性を確保，確認するプロセスを確立しました。第二世代デジタル安全系の一部は既に国内の原子力発電プラントに数多く適用しており，良好な運転実績を示しています。

当社は，第二世代と第一世代のデジタル安全系，更に，必要に応じて従来のハードワイヤード回路を組み合わせることで，多様化に対する要求事項を満足できると考えています。

現在設計を進めている米国向けABWR（改良型沸騰水型原子炉）には，当社の第二世代デジタル安全系と，米国で認可され実績がある東芝グループのウェスチングハウス社製の第一世代デジタル安全系を組み合わせたシステムを提案しています。米国向けABWRは既にNRCの型式認定を取得しており，現在，この実績に基づき提案したシステムについてNRCの審査を受けていますが，これまで改善すべき大きな指摘は受けておらず，予定どおりの審査合格を見込んでいます。

第三世代デジタル安全系に向けて

世界における今後の原子力発電プラントの建設増加を考慮すると，規制側，申請者側ともに審査負荷を軽減し，短期間での許認可の取得や工期の短縮を図ることが重要です。

そのために当社は，BWRとPWR（加圧水型原子炉）両方に適用可能で，共通した設計思想と標準化に基づく第三世代のデジタル安全系の開発に着手しています。第三世代デジタル安全系では，ウェスチングハウス社の経験や技術とのシナジーを生かし，信頼性の高いシステムが容易に構築できるよう，システム実現形態の柔軟化と設計の標準化を更に進めるとともに，システムV&Vやトレーサビリティ確認の負荷軽減のために，開発や試験のプロセスを改善します。

今後の展望

当社は今後，各国の規制状況に合致し，安全性や信頼性の維持向上に加え審査負荷の軽減や工期の短縮に貢献できる，デジタル安全系の最適ソリューションを提案し，地球環境問題に対する原子力発電への世界的な期待に応えていきます。

福本　亮
電力システム社
原子力事業部技監