

ディジタル安全保護系のソフトウェア共通要因故障問題の動向

Treatment of software common cause failure issue in digital reactor protection system

*内海 正文¹

¹三菱重工

原子力発電所の安全保護系へのディジタル制御装置の適用が進むなかで、制御ソフトウェアに起因する共通要因故障の取扱いが検討されており、発生防止、影響評価、対策検討を総合的に進める必要がある。

キーワード：安全保護系，ディジタル制御装置，ソフトウェア，共通要因故障

1. 緒言

原子力発電所の安全保護系にはディジタル制御装置の適用が進んでいるが、制御ソフトウェアに起因する共通要因故障（以下ソフトウェア共通要因故障）の影響評価と対策検討が求められている。

2. 共通要因故障対策の考え方

2-1. 国際的な検討動向

欧米を中心にソフトウェア共通要因故障の影響評価と対策に関する要求事項が検討されており、特に米国においては 1990 年代から規制化を始め、現在も規制内容の見直しや体系化を進めている。

2-2. 発生防止

ソフトウェア共通要因故障によって安全保護系が作動不能となるためには、ソフトウェア設計時に欠陥が作りこまれるとともに、何らかの要因でこの欠陥が実行されて故障状態として顕在化し、かつこのことが外部からは発見できないことが必要である。従来から設計時の欠陥排除のためのソフトウェア設計のシンプル化・可視化・検証の徹底や、ソフトウェア実行環境のシンプル化・堅牢化、自己診断機能の充実などが図られてきた。

2-3. 影響評価

ソフトウェア共通要因故障によって安全保護系がどのような範囲でどのような故障モードとなるのかを分析したうえで、この状態で過渡・事象が生じた場合のプラント安全性への影響を評価し、対策の要否を検討する必要がある。ソフトウェアの信頼性や共通要因故障の程度を定量的に評価することは困難ではあるが、決定論的な安全評価や P S Aなどを組み合わせて影響の範囲や程度を分析し、対策の要否を検討する必要がある。

2-4. 対策検討

ソフトウェア共通要因故障が生じたときの対策として、過渡・事象に対応する機能をバックアップする設備であって、安全保護系のソフトウェア共通要因故障の影響を受けないものを追加設置することが考えられるが、安全保護系本来の機能を阻害しないこと、運転操作に混乱を招かないことが必要である。

3. 結論

安全保護系へのディジタル制御装置の適用に際しては、国際的な検討動向との協調を図りながら、発生防止・影響評価・対策検討の総合的な対応が必要である。

*Masafumi Utsumi¹

¹Mitsubishi Heavy Industries, Ltd