参考１

発電用原子炉施設におけるデジタル安全保護系のソフトウェアに起因する共通要因故障対策について
～　多様化設備に係る要求事項の整理　～

令和元年10月30日
原子力規制庁

1. 背景と経緯

- 本年の原子力規制委員会の重要課題として、『発電用原子炉施設のデジタルI&C問題（デジタル安全保護系の共通要因故障対策）の規制への取り込み』が挙げられている。
- デジタル安全保護回路のソフトウェアに起因する共通要因故障対策については、第29回原子力規制委員会において今後の取組方針が了承され、最近の国際的な動向も踏まえ、信頼性向上の観点から現行規制の見直しを検討することとなった。
- 第33回原子力規制委員会において本検討チームの設置が了承され、検討チーム会合にはATENAや事業者、メーカー等の参加を求め、本件課題に関する事業者の意見や最近の動向等を聴取することとなった。

2. 検討の方向性

- 本検討チームでは、デジタル安全保護回路のソフトウェアに起因する共通要因故障対策として、次に掲げる方針で規制要求の具体化・整理等を進める。

① デジタル制御方式の安全保護回路を設ける場合には、ソフトウェア起因の共通要因故障対策として、デジタル安全保護回路とは動作原理の異なる別の手段（多様化設備）を設けるよう新たに要求することとし、許可段階からその基本設計方針を確認する。

② 多様化設備は、運転時の異常な過渡変化又は設計基準事故の発生時に、ソフトウェア起因の共通要因故障※によりデジタル安全保護回路が機能喪失すると仮定しても、発電用原子炉施設の安全性が損なわれることを防止することができるものとすることを要求する。

（※）安全評価上想定する単一故障ではない。

"COMMON POSITION ON THE TREATMENT OF COMMON CAUSE FAILURE CAUSED BY SOFTWARE WITHIN DIGITAL SAFETY SYSTEMS" (MDEP Generic Common Position No DICWG-01)

3. デジタル安全保護回路の定義

デジタル安全保護回路とは、安全保護回路のうち、ソフトウェア（電子計算機に対する指令であって、一の結果を得ることができるように組み合わされたものをいう。）を用いることによりその安全保護機能の全部又は一部を作動させるものをいう。

※参考※
「安全保護回路」とは、運転時の異常な過渡変化及び設計基準事故を検知し、これらの事象が発生した場合において原子炉停止系統及び工学的安全施設を自動的に作動させる設備をいう。（許可基準規則第2条第2項第40号）

⇒ 現行の許可基準規則第24条第3号及び第7号で、無定義で用いられている「安全保護機能」について、『運転時の異常な過渡変化及び設計基準事故の発生を検知し、原子炉停止系統及び工学的安全施設を自動的に作動させる機能をいう。』といった定義規定を追加して明確化する。

4. 多様化設備の設置要求

デジタル安全保護回路を設ける場合には、代替作動機能を有する装置（多様化設備）を設けなければならない。

【補足】

但し、安全保護機能の一部がソフトウェアにより作動するものである場合であって、当該ソフトウェアがその使用目的に沿うべき動作を電子計算機にさせることができない場合を仮定しても多様化設備を用いることなく判断基準を満足することが最適評価により確認できる場合には、多様化設備を設けなくても良い。

5. 多様化設備の要求事項:①想定事象

要求事項:①想定事象

運転時の異常な過渡変化又は設計基準事故(いずれも全事象)が発生したとき、すなわち、安全保護回路の自動作動が要求されたときに、ソフトウェアに起因する共通要因故障により安全保護機能が喪失するものと仮定する。

【補足】

運転時の異常な過渡変化又は設計基準事故が発生した場合において、デジタル安全保護回路がその異常な状態を検知することできないとき又は原子炉停止系統及び工学的安全施設を自動的に作動させることができないときを仮定する。

5. 多様化設備の要求事項:②代替作動機能

要求事項:②代替作動機能

ソフトウェア起因の共通要因故障により、多重化されたデジタル安全保護回路がその安全保護機能を喪失した場合において、

A) 安全保護回路とは異なる動作原理の機構により、

B) 原子炉停止系統及び工学的安全施設を

C) 自動的に、又は原子炉制御室から手動により作動させることができること。

【補足】
「A)安全保護回路とは異なる動作原理の機構」とは、ソフトウェアを用いることなく作動させることができるものなど、ソフトウェアに起因する共通要因故障によってデジタル安全保護回路と同時にその機能を喪失するおそれがないものをいう。

5. 多様化設備の要求事項:③信頼性

要求事項:③信頼性

共通要因によって安全保護回路の安全保護機能と同時にその代替作動機能が損なわれるおそれがないよう、適切な措置を講じたものとすること。

【補足】
「適切な措置を講じたもの」とは、安全保護回路の作動が要求される場合において安全保護機能と代替作動機能とが同時に損なわれないよう、物理的方法その他の方法によりそれぞれ互いに分離することをいう。

設計基準事故等の起因となる事象に対して、その起因事象の影響を考慮しても安全保護機能に期待することなく多様化設備により適切に対処できるよう設計すること。
例えば、ある想定される火災区域での火災により設計基準事故等が発生する場合には、その火災に対して安全保護回路と多様化設備が同時に機能喪失しないよう設計すること。

5. 多様化設備の要求事項:③信頼性 （つづき）

要求事項:③信頼性 （つづき）

外部電源が利用できない場合においてもその代替作動機能が損なわれるおそれがないものとすること。

許可基準規則第3条【地盤】、第4条【地震】、第5条【津波】、第6条【外部事象】、第8条【内部火災】、第9条【溢水】、第10条【誤操作】、第12条【安全施設】、第33条【保安電源】の各規定を適用又は準用する。

【補足】
なお、第12条【安全施設】のうち、第2項（多重性又は多様性及び独立性）については、同旨の要求内容を別に規定するため、適用しない。

6. 多様化設備の成立性の確認

①評価方法

運転時の異常な過渡変化又は設計基準事故が発生し、かつ、安全保護回路の安全保護機能が喪失すると仮定した場合でも、多様化設備が有効に機能することにより炉心損傷を防止できることを最適評価により確認する。

【補足】
安全評価（添十解析）とは異なり、最適評価により炉心損傷を防止できることを確認する。この際、以下を考慮しても良い。

a. 安全保護回路は機能喪失するが、原子炉停止系統及び工学的安全施設は利用可能。
b. 多様化設備の単一故障は仮定しない。
c. 運転員による現場操作を想定して良い。
d. 運転員の事態認知から手動操作までの時間など、評価に用いるモデルやパラメータ等は現実的なもので良い（いわゆる10分ルールは適用しない）。

6. 多様化設備の成立性の確認 （つづき）

②判断基準

運転時の異常な過渡変化又は設計基準事故が発生し、かつ、安全保護回路の安全保護機能が喪失すると仮定した場合でも、炉心損傷を防止できるものとすること。

【補足】
「炉心損傷を防止できる」とは、多様化設備が有効に機能することにより、許可基準規則第13条第2号の要件（DBAの判断基準）を満足することをいう。

7. 事業者意見の聴取

事業者意見（経過措置に関するものを含む。）がある場合には、第3回検討チーム会合で聴取し、科学的・技術的な観点から議論する。なお、有意義な議論を行うため、意見にはその理由を付するとともに、それらの科学的・技術的な妥当性等を確認・検証することができる文献・データ等を添付して、書面により提出することを推奨する。