柏崎刈羽原子力発電所 7 号機

デジタル安全保護回路のソフトウェア共通要因
故障緩和対策に関する要件整合確認書
(手順書)
(改訂 1)

2025年 3月13日
原子力エネルギー協議会

改訂履歴

改訂番号	改訂年月	改訂内容	備考
初版	2023年7月14日	新規作成	—
1	2025年3月13日	・多様化設備の警報回路内のタイマーリレー内部にワンチップマイコンが使用されていることを受けた手順書改訂に係る整合確認を反映	—

1. はじめに

東京電力ホールディングス(株)は、柏崎刈羽原子力発電所 7 号機のデジタル安全保護回路のソフトウェア共通要因故障緩和対策(以下、「デジタル CCF 対策」という。)に係る安全対策に関して、技術要件書*の「5. 手順書の整備と教育及び訓練の実施」の各要求内容に整合しているかの確認を行い、2023 年 7 月 6 日に「柏崎刈羽原子力発電所 7 号機デジタル安全保護回路のソフトウェア共通要因故障緩和対策に関する要件整合報告書(手順書)(以下、「要件整合報告書(手順書)」という。)」を ATENA に提出した。

ATENA は、受領した要件整合報告書(手順書)の確認を行い、確認結果を 2023 年 7 月 14 日に要件整合確認書として取りまとめた。

※原子力発電所におけるデジタル安全保護回路のソフトウェア共通要因故障緩和対策に関する技術要件書(ATENA 20-ME05 Rev.1)

その後、多様化設備の警報回路内(ARI 作動(ハード), L-2(ハード), 原子炉圧力高高(ハード))のタイマーリレー内部にワンチップマイコンが使用されていることが判明したため、東京電力ホールディングス(株)は、ソフトウェア CCF 発生時に当該タイマーリレーの動作を期待できないことを考慮した場合でも運転員が事象に対応可能なように手順書に注記を追加する改訂を行った。そして、改訂部分について最新の技術要件書*の各要求内容に整合しているかの確認を行い、2025 年 2 月 28 日に要件整合報告書(手順書)(改訂1)を ATENA に提出した。

ATENA は、受領した要件整合報告書(手順書)(改訂1)の確認を行い、確認結果を本要件整合確認書として取りまとめた。

※原子力発電所におけるデジタル安全保護回路のソフトウェア共通要因故障緩和対策に関する技術要件書(ATENA 20-ME05 Rev.2)

なお、今回の改訂は、下記に示す技術要件書の解説 3.5.2 の記載を踏まえて、デジタル機器と判断される当該タイマーリレーに対して、ソフトウェア CCF 発生時に当該タイマーリレーの動作を期待できないことを考慮し、その場合でも運転員が事象に対応可能なように手順書に注記を追加したものである。

(技術要件書 解説 3.5.2 抜粋)

「多様化設備に適用するデジタル技術の要件が定まるまでは、多様化設備の一部に FPGA 等のデジタル機器を使用する場合には、当該デジタル機器の影響を受ける機能について、多様化設備としての動作を期待できないことを考慮する必要がある。」

2. 確認方法

「柏崎刈羽原子力発電所 7 号機 デジタル安全保護回路のソフトウェア共通要因故障緩和対策に関する要件整合報告書(詳細設計)(以下、「要件整合報告書(詳細設計)」という。)」に示された設備設計、及び有効性評価で想定した手段と運転操作条件が手順書に記載されており、その手順書に基づき運転員の習熟を図る教育及び訓練計画が定められていることを確認する。

具体的には、受領した要件整合報告書(手順書)及びそのエビデンス(手順及び教育訓練に係る規定文書)に対して、表1に示す確認内容及び確認の観点に基づき、技術要件書の「5. 手順書の整備と教育及び訓練の実施」の各要求内容に対する整合性の確認を行う。

なお、今回(改訂1)の要件整合確認における確認体制及び確認フローについて、添付資料1に示す。

また、今回(改訂1)の要件整合確認にあたり参照した最新の技術要件書(ATENA 20-ME05 Rev.2)は、技術要件書(ATENA 20-ME05 Rev.1)から表現改善、参考情報の追加の変更を行っているが、要求内容には変更がないことから、確認はワンチップマイコンが使用されているタイマーリレーの機能喪失を考慮した場合にソフトウェア CCF 事象の発生を認知する手順に係る範囲のみを対象とした。

表1 要件整合確認(手順書)における確認内容及び確認の観点

技術要件書の要求	確認内容	確認の観点
5.1 手順書の整備	デジタル安全保護回路の自動作動が要求されたときに原子炉停止系統及び工学的安全施設が作動していないことを認知する手段を特定し、ソフトウェアCCF事象を判断する手順が記載されていること。	① デジタル安全保護回路の自動動作が要求される状況において、デジタル安全保護回路が作動せずに多様化自動作動設備の自動作動や警報発信によってソフトウェア CCF 事象の発生を認知する手段と手順が記載されているか。
	所定の手順に移行する方法が明確になっていること。	② ソフトウェア CCF 事象の発生を認知し、所定の手順に移行する方法が記載されているか。
	運転操作を行う場合の判断条件及び操作場所が記載されていること。	③ 運転操作を行う場合の手段(自動作動機能、手動機能、警報機能、指示機能)とその判断条件(設定値や状態表示)及び操作・監視を行う場所(盤略号など)が記載されているか。
	プラント状態を監視するための手段及びその設置場所が記載されていること。	④ 原子炉停止系統及び工学的安全施設の作動状況、多様化自動作動設備の作動状況及び手動操作によるプラント状態を監視するための手段(警報機能、指示機能など)及び監視を行う場所(盤略号など)が記載されているか。
5.2 教育及び訓練の実施	運転員に対して、整備された手順書の内容について習熟を図ることができるよう、教育及び訓練が計画されていること。	⑤ デジタル安全保護回路のソフトウェア CCFの対応について運転員の習熟を図る教育及び訓練計画が記載されているか。

3. 要件整合確認結果

手順書の整備と教育及び訓練の実施に対する要件整合性について、技術要件書の「5.1 手順書の整備」及び「5.2 教育及び訓練の実施」の各要求内容に対して、表1に示す確認内容及び確認の観点に基づき、今回の改訂箇所に係る要件整合報告書(手順書)及び表 2 に示すエビデンス(手順及び教育訓練に係る規定文書)の内容を確認した。

各要求内容に対する確認結果については表 3 に示す。

表 2 エビデンス(手順及び教育訓練に係る規定文書)

	規定文書(改訂箇所)	添付資料番号
手順に係る 規定文書	警報発生時操作手順書 ・ARI 作動(ハード) ・L-2(ハード) ・原子炉圧力高高(ハード)	添付資料 2

(1)「5.1 手順書の整備」について

警報発生時操作手順書、事故時運転操作手順書(徴候ベース)及び・設備別操作手順書に以下の内容が記載されていることを確認した。

- ・ 運転時の異常な過渡変化又は設計基準事故が発生し、デジタル安全保護回路の自動作動が要求される状況において、デジタル安全保護回路が作動せずに多様化自動作動設備の自動作動や警報発信によってソフトウェア CCF 事象の発生を認知する手順が記載されていること。このとき、ワンチップマイコンが使用されているタイマーリレーの機能喪失を考慮した場合についてもソフトウェア CCF 事象の発生を認知する手順が記載されていること。
- ・ ソフトウェア CCF 事象の発生を認知し、警報発生時操作手順書による運転操作を行い、原子炉スクラムが発生している場合には事故時運転操作手順書(徴候ベース)「スクラム」へ移行する方法が記載されていること。
- ・ ソフトウェア CCF 事象により、中央制御室からの遠隔操作が不能となった場合には設備別操作手順書のデジタル安全保護回路(ソフトロジック)を使用しない手動操作へ移行する方法が記載されていること。
- ・ 運転操作を行う場合の判断条件及び操作場所が記載されていること。
- ・ プラント状態を監視するための計器及びその設置場所が記載されていること。
- ・ 上記のソフトウェア CCF 事象発生の認知、運転操作及びプラント状態の監視に関して、必要な手段として添付資料 3 に示す要件整合報告書(詳細設計)の別表 1 から別表 4 の機能(自動動作機能、手動作動機能、警報機能、指示機能)が操作場所(盤略号など)も含めて記載されていること、及び有効性評価で想定した運転操作開始や機器状態等の運転操作条件が記載されていること。

以上のことから、運転時の異常な過渡変化又は設計基準事故にソフトウェア CCF が重畳したことを判断した上で、必要な運転操作を実施し、判断基準を概ね満足した状態で事象を収束するための手順書が整備されていることを確認した。

(2)「5.2 教育及び訓練の実施」について

教育及び訓練に関しては、原子力発電所運転員に対する教育・訓練マニュアル及び原子力発電所運転員のシミュレータ訓練実施ガイドにおいて、従来の事故時の手順書と同じ教育訓練体系の中にデジタル CCF 対策として整備した手順書の訓

練が追加されており、対象者及び実施頻度についても従来の事故時の手順書と同じく管理されることは 2023 年 7 月 14 日の要件整合確認書において確認されている。

以上のことから、整備された手順書に従いた的確な対処をするために必要な力量を付与させるための教育及び訓練を、その対象者及び実施頻度を含め適切に計画し、実施することが規定されていることを確認した。

4. まとめ

柏崎刈羽原子力発電所 7 号機 の要件整合報告書(手順書)は、技術要件書の「5. 手順書の整備と教育及び訓練の実施」の各要求内容に対して全て整合していることを確認した。

5. 添付資料

添付資料 1 要件整合確認における確認体制及び確認フロー

添付資料 2 柏崎刈羽原子力発電所 7 号機 要件整合報告書(手順書)(改訂1)
添付資料(抜粋)

表3 デジタル安全保護回路のソフトウェア共通要因故障緩和対策に関する要件整合確認結果
【対象：柏崎刈羽原子力発電所7号機（手順書）】

ATENA 技術要件書	事業者の要件整合報告の内容			ATENA による要件整合確認結果
	記載内容(概要)	要件整合性		
要求内容		判定	理由	
5.1 手順書の整備				
<p>運転時の異常な過渡変化又は設計基準事故が発生した際に、デジタル安全保護回路の安全機能の喪失によって、原子炉停止系統及び工学的安全施設が自動作動していないことを運転員が認知した場合に、その要因がソフトウェア CCF の重畳によることを判断した上で、必要な運転操作を実施し、判断基準を概ね満足した状態で事象を収束することができるための手順書を整備すること。なお、有効性評価により多様化設備の設置が不要であることが確認された場合は、多様化設備を用いた手順書の整備は不要である。その場合、ソフトウェア CCF の影響を受ける事象 に対して、その原因がソフトウェア CCF と認知できずとも、現行の運転手順書にて、ソフトウェア CCF の影響を受けない他の計器や警報により異常の発生を認知し、必要な運転操作を行うことが可能であることを確認すること。</p>	<p>ソフトウェア CCF 対策の手順書の整備については、運転時の異常な過渡変化又は設計基準事故にソフトウェア CCF が重畳した事象を想定(デジタル安全保護系は全ての機能が喪失する)し、運転員の必要な操作により事象を収束する手順書を整備した。</p> <p>なお、当該手順書は、運転時の異常な過渡変化又は設計基準事故とソフトウェア CCF の発生が重畳したことを判断した結果から、所定の手順に移行する方法を記載した手順書、及びソフトウェア CCF 発生時の個別操作を記載した手順書であり、具体的には、以下の内容を手順書に整備した。</p> <p>1. 警報発生時操作手順書 ARI 作動(ハード)、L-2(ハード)、原子炉圧力高高(ハード) ・デジタル安全保護回路の安全機能が喪失し、デジタル安全保護回路から原子炉停止系統及び工学的安全施設が自動作動していないことを、通常の警報が発信されないこと及び多様化設備の警報が発信することの比較により運転員が判断する。 ・ソフトウェア CCF 時に想定する事象に対応するための以下の手順のいずれかに移行し、必要な運転操作(手動操作、現場操作)を行う。 事故時運転操作手順書(徴候ベース) 設備別操作手順書 ・ソフトウェア CCF の発生形態によっては、CCF 事象発生時に多様化設備の警報窓のランプが点滅せず、ホーンのみが鳴動する場合がある旨 と、その場合の対応 を明記している。</p>	<p>○</p> <p>以下の手順が規定文書に定められていることを確認した。</p> <ul style="list-style-type: none"> ・運転時の異常な過渡変化又は設計基準事故が発生した際に、デジタル安全保護回路の安全機能が喪失していることを、原子炉停止系統及び工学的安全施設等が自動作動していないこと及び多様化自動作動設備の警報により認知できること。 ・上記よりソフトウェア CCF の重畳によることを判断した上で、所定の運転操作を実施する手順に移行することが明確になっていること。 ・判断基準を概ね満足した状態で事象を収束することができるよう、有効性評価で想定している運転操作条件を考慮した手順となっていること。 ・「柏崎刈羽原子力発電所7号機 デジタル安全保護回路のソフトウェア共通要因故障緩和対策に関する要件整合報告書(詳細設計)」の「3.2 機能要求」で確認した自動作動機能、手動機能、警報機能及び指示機能について、手順に反映されており、運転操作を行う条件(運転操作の開始や機器状態など)及び操作場所(盤略号など)が明確化されていること。 ・ワンチップマイコンが使用されているタイマーリレーの機能喪失を考慮した場合でも、運転員がソフトウェア CCF を認知可能な手順書となっていること。 	<p>警報発生時操作手順書</p> <ul style="list-style-type: none"> ・ARI 作動(ハード) ・L-2(ハード) ・原子炉圧力高高(ハード) 	<p>① 運転時の異常な過渡変化又は設計基準事故が発生し、デジタル安全保護回路の自動作動が要求される状況において、デジタル安全保護回路が作動せずに多様化自動作動設備の自動作動や警報発信によってソフトウェア CCF 事象の発生を認知する手順が記載されていることを確認した。</p> <p>具体的には、ソフトウェア CCF 事象発生時の認知のための手段として要件整合報告書(詳細設計)の別表1から4の機能(自動作動機能、手動機能、警報機能、指示機能)が具体的に記載されていることを確認した。</p> <p>今回の手順書改訂にあたっては、ワンチップマイコンが使用されているタイマーリレーの機能喪失を考慮した場合についてもソフトウェア CCF 事象の発生を認知する手順が注記されていることを確認した。(その他の整合性は 2023 年 7 月 14 日の要件整合確認書において確認済み。)</p> <p>【確認資料】</p> <ul style="list-style-type: none"> ・警報発生時操作手順書

表3 デジタル安全保護回路のソフトウェア共通要因故障緩和対策に関する要件整合確認結果
【対象：柏崎刈羽原子力発電所7号機（手順書）】

	<p>2. 事故時運転操作手順書(徴候ベース)</p> <ul style="list-style-type: none"> デジタル安全保護回路の安全機能が喪失し、デジタル安全保護回路から原子炉停止系統及び工学的安全施設が自動作動していないことを、警報発生時操作手順書により運転員が判断した場合に、警報発生時操作手順書から移行し、事象を収束させるために必要な運転操作を行う。 <p>3. 設備別操作手順書</p> <ul style="list-style-type: none"> ソフトウェア CCF 時に期待する設備のサポート系空調、及び非常用ディーゼル発電機の自動起動に失敗した場合に、必要な運転操作(手動操作、現場操作)を行う。 	○		<p>事故時運転操作手順書(徴候ベース)</p> <ul style="list-style-type: none"> フローチャート HPCF(C)手動起動確認シート <p>【格納容器補助盤用】</p> <ul style="list-style-type: none"> HPAC起動確認シート <p>設備別操作手順書</p> <ul style="list-style-type: none"> 4-1項 原子炉区域ローカル換気空調設備の手動操作 4-2項 海水熱交換器建屋換気空調設備の手動操作 4-3項 D/G区域換気空調設備の手動操作 4-4項 コントロール建屋換気空調設備の手動操作 4-5項 換気空調補機非常用冷却設備の手動操作 4-6項 中央制御室系換気空調設備の手動操作(事故時切替操作含む) 4-7項 非常用ディーゼル発電設備の手動操作 	<p>② ソフトウェア CCF 事象の発生を認知し、警報発生時操作手順書による運転操作を行い、原子炉スクラムが発生している場合には事故時運転操作手順書(徴候ベース)「スクラム」へ移行する方法が記載されていることを確認した。</p> <p>また、ソフトウェア CCF 事象により、中央制御室からの遠隔操作が不能となった場合には設備別操作手順書のデジタル安全保護回路(ソフトロジック)を使用しない手動操作へ移行する方法が記載されていることを確認した。</p> <p>【確認資料】</p> <ul style="list-style-type: none"> 警報発生時操作手順書 事故時運転操作手順書(徴候ベース) <p>③ 設備別操作手順書運転操作を行うための手段(自動作動機能、手動機能、警報機能、指示機能)、運転操作を行う条件(運転操作の開始や機器状態など)及び操作・監視する機器の設置場所(盤略号など)が記載されていることを確認した。</p> <p>【確認資料】</p> <ul style="list-style-type: none"> 警報発生時操作手順書 事故時運転操作手順書(徴候ベース) <p>④ プラント状態を監視する手段(警報機能、指示機能)及び監視する機器の設置場所(盤略号など)が記載されていることを確認した。</p> <p>【確認資料】</p> <ul style="list-style-type: none"> 警報発生時操作手順書 <p>(整合性は2023年7月14日の要件整合確認書において確認済み。)</p>
--	--	---	--	--	--

表3 デジタル安全保護回路のソフトウェア共通要因故障緩和対策に関する要件整合確認結果
 【対象：柏崎刈羽原子力発電所7号機（手順書）】

(判定記号) ○：整合性有 -：該当なし

ATENA 技術要件書	事業者の要件整合報告の内容			ATENA による要件整合確認結果	
	記載内容(概要)	要件整合性			規定文書
		判定	理由		
要求内容				表1に示す確認内容及び確認の観点に基づき確認 ①～⑤の番号は表1の確認の観点の番号	
5.2 教育及び訓練の実施					
<p>運転員には、運転時の異常な過渡変化又は設計基準事故とソフトウェア CCF が重畳する事象に対して、整備された手順書に従った適切な対応をするために必要な力量を付与させるための教育及び訓練を、その対象・実施頻度を含め適切に計画し、実施すること。なお、多様化設備の設置が不要で現行の運転手順書にて、必要な運転操作を行うことが可能な場合には、ソフトウェア CCF の知見に関する教育を、その対象・実施頻度を含め適切に計画し、実施すること。</p>	<p>ソフトウェアCCFに係る教育及び訓練については、運転時の異常な過渡変化又は設計基準事故とソフトウェア CCF が重畳する事象に対して、整備された手順書に従った適切な対応をするために教育及び訓練を実施する計画(対象者、頻度)を整備した。</p>	○	<p>運転時の異常な過渡変化又は設計基準事故とソフトウェア CCF が重畳する事象に対して整備した手順書に従った適切な対応をするため、運転員に対し、必要な力量を付与する教育及び訓練(実施頻度含む)を適切に計画・実施することが規定文書に定められていることを確認した。</p>	<p>原子力発電所運転員に対する教育・訓練マニュアル ・別表 1-2 ・別表 2-1 原子力発電所運転員のシミュレータ訓練実施ガイド</p>	<p>⑤ 従来の事故時の手順書と同じ教育訓練体系の中に今回整備した手順書の訓練が追加されており、対象者及び実施頻度についても従来の事故時の手順書と同じく管理されることを確認した。 【確認資料】 ・原子力発電所運転員に対する教育・訓練マニュアル(別表 1-2、別表 2-1) ・原子力発電所運転員のシミュレータ訓練実施ガイド(整合性は2023年7月14日の要件整合確認書において確認済み。)</p>

要件整合確認における確認体制及び確認フロー

要件整合確認(改訂1)における確認体制及び確認フロー

1. 確認体制

今回の要件整合確認は、下表に示す ATENA 確認チームにて実施した。

なお、ATENA 確認チームの人選にあたっては、当該プラントのデジタル CCF 対策設備の詳細設計、有効性評価、手順書整備などに直接関わっていないことを条件に、業務経歴をもとに力量を確認した。

表 ATENA 確認チーム

	氏名	所属・役職
責任者	■■■■■	原子力エネルギー協議会 技術班 部長
担当者	■■■■■	原子力エネルギー協議会 運営班 副部長

2. 確認フロー

今回の要件整合確認にあたっては、以下のフローで実施した。

- ATENA-WG(デジタル CCF-WG)にて要件整合報告書(手順書)(改訂1)の改訂に係る記載内容や様式の検討を行った。手順書改訂による処置の妥当性については、専門家(デジタル CCF-WG メンバー)による第三者レビューを実施し、内容に問題がないことを確認した。その検討結果をもとに事業者は要件整合報告書(手順書)を取りまとめ、ATENA に提出した。
- ATENA は、受領した要件整合報告書(手順書)(改訂1)及び改訂に係るエビデンス(手順及び教育訓練に係る規定文書)の記載内容について、ATENA 確認チームによる要件整合確認を行った。
- ATENA 確認チームは、要件整合確認結果を ATENA 役員に報告し、承認を得た。

柏崎刈羽原子力発電所 7 号機 要件整合報告書
(手順書) (改訂1)

添付資料(抜粋)

柏崎刈羽原子力発電所 7 号機

デジタル安全保護回路の
ソフトウェア共通要因故障緩和対策に関する
要件整合報告書(手順書)

2025 年 2 月 28 日

東京電力ホールディングス株式会社

Ⅱ. 添 付 書 類

目 次

(1) 添付資料

添付1 柏崎刈羽原子力発電所7号機 警報発生時操作手順書

添付1-1 ARI 作動(ハード)

添付1-2 L-2(ハード)

添付1-3 原子炉圧力高高(ハード)

(1) 添付資料

添付1 柏崎刈羽原子力発電所7号機 警報発生時操作手順書

本資料は、機密に係る情報のため公開できません

添付1-1 ARI 作動(ハード)

本資料は、機密に係る情報のため公開できません

添付1-2 L-2(ハード)

本資料は、機密に係る情報のため公開できません

添付1-3 原子炉圧力高高(ハード)

本資料は、機密に係る情報のため公開できません