

ドラフト

「安全保護系へのデジタル計算機の適用に関する規程に関する
日本電気協会への説明依頼事項(案)」に対する回答

令和4年●月●日
(一社)日本電気協会
原子力規格委員会

標記につきましては、以下の通り回答いたします。

○説明依頼事項

1. 2008年版では「4.7 試験可能性」に「原子炉運転中でも試験ができる機能を有する設計とすること。」と規定されたものが、2020年版では「原子炉運転中でも各チャンネルが独立に試験ができる設計とすること。」¹と変更されています。「試験ができる機能を有する設計」を「試験ができる設計」に変更した理由について説明して下さい。
※ 「試験ができる機能」を有する設計とは、例えば、試験を開始するための操作スイッチを有する設計が考えられます。
2. 「(解説-19) ソフトウェアライフサイクル」の「(2)各プロセスで実施すべき品質管理項目」の「(f)変更プロセス」に規定する「ソフトウェアの変更要否について調査する。」に対するV&Vは行うのか、行う場合に検証と妥当性確認のどちらに区分するとしているのか、説明して下さい。

¹ 「4.8 試験可能性」参照

○回答

1. 2008年版では「4.7 試験可能性」に「原子炉運転中でも試験ができる機能を有する設計とすること。」と規定されたものが、2020年版では「原子炉運転中でも各チャンネルが独立に試験ができる設計とすること。」¹と変更されています。「試験ができる機能を有する設計」を「試験ができる設計」に変更した理由について説明して下さい。

※ 「試験ができる機能」を有する設計とは、例えば、試験を開始するための操作スイッチを有する設計が考えられます。

回答 1)

「試験ができる設計」と「試験ができる機能を有する設計」に要求上の差異はなく、言葉の重複を避けたものです。つまり「〇〇できる」ということは、「〇〇の機能を有する」と同義であると考えています。

また、参考としている基準類や IEEE においても、文章の根幹だけを抜き出すと「試験ができる設計(もの)とする」あるいは「Capability of testing shall be provided(試験可能性を有すること)」となります。

なお、試験のための切り替えスイッチや試験端子を設けることは、試験できる設計を実装する際の技術的な選択枝のひとつですが、試験を行うためには安全保護系以外の装置(信号発生器やテスターなど)も必要であることから、安全保護系の中に試験が実施できる機能をすべて持たせるものではありません。

2. 「(解説-19) ソフトウェアライフサイクル」の「(2)各プロセスで実施すべき品質管理項目」の「(f)変更プロセス」に規定する「ソフトウェアの変更要否について調査する。」に対するV&Vは行うのか、行う場合に検証と妥当性確認のどちらに区分するとしているのか、説明してください。

回答 2)

変更プロセスの「ソフトウェアの変更要否について調査する」プロセスは設計・製作者が行いますが、このプロセスそのものに対してV&Vは行いません。

変更の決定を受けて、変更内容は設計・製作の図書に反映されますので、V&V実施者はそれらの図書に対してV&Vを行います。例えば変更箇所が上位図書の要件から相違がないことの検証等を含めて確認しています。V&Vによって変更内容が上位図書の要件に不適切であることが分かった場合などには設計・製作者に対して是正を求めることとしています。