

機能安全への取り組み

(株)ヴィッツ 森川 聡久

社内では機能安全業務をかれこれ4年近く担当しています。2010年4月に日本初のIEC61508プロセス認証を取得することができました！！今では、色んな企業様の機能安全対応を支援させていただいています。

■機能安全支援について

・機能安全管理規定の作成支援

機能安全管理規定とは、ISO9000など品質管理の機能安全版です。

規定の作成支援や、プロセス認証取得支援ができます。

プロセス認証を取得するには、組織が実施できることを示す必要があります。

・安全設計、安全分析支援

安全なアーキテクチャ設計、FMEA/HAZOPなど安全分析の実施を支援します。

機能安全では、安全なシステムだ！という「安全証明」が必要です。

・SIL (Safety Integrity Level) 算出評価

安全設計したシステムについて、SILいくつくらいのレベルにあるのかを、算出評価します。開発完了したシステムについて、より正確な算出評価も可能です。

・機能安全対応のソフトウェア受託開発

認証取得した機能安全プロセスに従って、ソフトウェアの受託開発ができます。

・機能安全規格解説

機能安全に必要な作業内容を具体的に解説します。

規格書の記述は抽象的なので、意味を理解するのは非常に難しいです。また、誤った解釈をしてしまうと、やりすぎ（作業の無駄）や不足の恐れがあります。

・機能安全認証取得支援

規格書に書いてあるように実施すれば、簡単に認証なんて取れる！そう思われるかも知れませんが、実際は違います。認証官が理解できないことには、認証なんて取得できませんから。

認証官との対応のやり方次第で、時間もお金も何倍も違ってきます。低コストで対応できるノウハウをお教えします。

■従来開発と機能安全開発

機能安全開発って別に特別なものではありません。日本企業は既に品質・安全へのケアをした開発をしています。きちんとした開発をしている企業様であれば、実はそこそこ対応できているかも知れません。

認証機関も、日本企業は機能安全対応を過剰にやりすぎている（やろうとしている）、と言っています。その一番の原因は、規格書に書いてあることをそのまま実施しようとするため。やりすぎは逆に危険です！無駄な作業が増えると、他の重要な作業がおろそかになる恐れがあるから。

かといって、薄っぺらなやり方でもダメです。要は、機能安全規格の「ココロ」を正しくつかむことが重要です。時間かかりますけど・・・。

■今年のSWESTは・・・

2日目の機能安全セッションにて、パネラーを務めさせていただきます。

また、懇親会、徹夜部屋などでも、機能安全に関するディスカッションができればと思います。

どうぞ宜しくお願いいたします。