安全性を主張する上で必要な独立性の割り当て

今回は、安全性を主張する上で必要な独立性の割り当てについてご紹介します。ISO 26262 のコンファメーションメジャーと呼ばれる各種活動では、安全性を主張する上で独立性が求められています。ここでいう各種活動とは、コンファメーションレビュー、機能安全監査、機能安全アセスメントの三種類の活動を指しており、製品開発のライフサイクルの中で適切なタイミングで組織の安全方針に基づいて、適切に計画される必要があります。

ISO 26262 では、対象となる成果物の作成者とコンファメーションメジャーの実施者の間の独立性が、それぞれのコンファメーションメジャーと ASIL の組み合わせによって、I0～I3 の四段階で要求されています。これらの I0～I3 の独立性は、何のために求められているのでしょうか。

まず、I0 と I1 における独立性は、コンファメーションメジャーの実施者と成果物の作成者が異なるということを求めています。これらは、成果物の作成者個人のヒューマンエラーや不正行為などに起因した問題の検出を期待します。実際のところ、このレベルの独立性においては、担当者間の人間関係などから、不正行為について指摘しにくい面もありますので、作成者個人の「うっかりミス」や「思い込み」などのヒューマンエラーを検出することを主な目的と考えていただいた方が良いと思います。なお、I0 と I1 の違いは、この独立性を適用することが「should：すべき」「shall：しなければならない」という要求の強さの違いになります。
次に I2 における独立性は、コンファメーションメジャーの実施者が成果物の作成者と異なるチームに属していることを求めています。これは、主にチーム内の固定概念に起因した問題や、チームとしての不正行為などに起因した問題の検出を期待します。ここで言う異なるチームとは、成果物の作成者が携わる開発プロジェクトからの独立性を指しており、同じ部署内であっても、担当するプロジェクトが異なっていれば、これに該当します。
もっとも厳しい I3 における独立性は、コンファメーションメジャーの実施者が成果物の作成者と異なる部署や組織に属していることを求めています。これは、I2 までの期待に加えて、対象の開発部署の制約（コスト、リソース、納期など）に起因した問題の検出と強い是正勧告を期待します。ここでいう強い是正勧告とは、ただ強く指摘するというだけではなく、問題解決に向けたアクションを起こすことが求められます。
たとえば、プロジェクトに割り当てられたリソースが不足しているために問題を解決できないのであれば、プロジェクトに対してリソースを新たに割り当てる必要があります。そのため、I3 では管理、リソース、納期に関する独立した権限を持つことが求められています。

たとえば、ある組織がソフトウエアツール認定報告のコンファメーションレビューを実施したとします。このケースにおいて、ISO26262 では、I1（ASIL D の場合）が求められていますが、このコンファメーションレビューを、I3 に該当する独立した品質管理部門の担当者が実施したとします。この場合、担当者の担当範囲外であり、ソフトウエアツールの想定されたユースケースと開発現場のユースケースの違いを判断することは対応出来ません。それにより、開発現場によるソフトウエアツールの想定外のユースケースを見落とすリスクが発生します。このような事が考えられるため、ソフトウエアツール認定報告に対して、I3 のコンファメーションレビューを実施することが、適切とはいえません。

このように安全性を主張する上で必要な独立性は、プロジェクトライフサイクルの中で各種活動における目的とそれを達成可能な独立性を考慮して設定し、安全活動へと割り当てることが重要です。
(2012 年 07 月号 メルマガ抜粋)

ビジネスキューブ・アンド・パートナーズ株式会社
東京都渋谷区広尾 1-13-1 フジキカイ広尾ビル 5F
TEL：03-5791-2121 / FAX：03-5791-2122 / E-mail：consulting@biz3.co.jp
URL：http://biz3.co.jp