# ISO 26262 に基づくダイアグカバレッジの見積もり方法とその重要性

## はじめに：規格が求める“論理的根拠”とは何か

ISO 26262 では、安全関連ハードウェアエレメントに対するセーフティメカニズムの有効性を、ダイアグカバレッジ（故障検出率）として定量的に評価することが求められています。
この評価は、残存フォールト（現時点で残っている故障）およびレイテントフォールト（潜在的に混入しうる故障）に対して行う必要があります。
では、その「論理的根拠」は、どのように示せばよいのでしょうか？
ここで誤解しがちなのが Part 5 Annex D の位置づけです。Annex D は“分析の出発点”であり、“根拠を示すもの”ではありません。規格は論理的根拠を明確に示す手段として、Part 10 の残存故障率評価や、Part 11 Annex A のセーフティメカニズムによるダイアグカバレッジの定量的評価例を挙げています。
Part 11 Annex A では、対象機能の故障モードごとにセーフティメカニズムの検出能力を検証し、数値として導出する方法が示されています。また、Part 5 7.4.3.3／7.4.3.4 では、「安全機構の有効性の証拠」をテスト・解析・シミュレーションなどで示すことが明文化されています。
では、実際に「ダイアグカバレッジの見積もり」とはどのような作業なのでしょうか？

## ダイアグカバレッジの見積もりとは

ダイアグカバレッジとは、安全関連ハードウェアエレメントの故障をセーフティメカニズムがどれくらい検出できるかを示す指標です。
ISO 26262 Part 5 8.4.2 では、この見積もりを通じて、システムの安全性を定量的に評価することが求められています。
システムの安全性を確保するためには、安全関連ハードウェアエレメントに対してどのようなセーフティメカニズムが必要か、そしてそれらがどの程度の故障を検出できるかを評価しなければなりません。
以降では、ダイアグカバレッジの見積もり方法とその重要性について、規格の要求と実践的なアプローチの両面からお話ししたいと思います。

## ダイアグカバレッジの定量的評価値を導く“4 ステップ”

実際にどのようなプロセスでダイアグカバレッジを導けば良いのでしょうか。
Part 11 Annex A では、DMA（Direct Memory Access）を例に、以下の 4 ステップが示されています。

1. ユースケースの整理
2. セーフティメカニズムの選定
3. 故障モードの定義
4. ダイアグカバレッジの計算

具体的には、通信ペリフェラルが一定周期でメッセージを受信し、DMA が固定 RAM へ転送、転送完了で CPU 割り込み、というシナリオをベースに、MPU・E2E プロテクション・Timeout 監視という 3 つのセーフティメカニズムを選定しています。
故障モードは「不実行」「不要実行」「タイミング異常」「不正な出力」の 4 つに大別して洗い出し、各々の故

障モードごとにセーフティメカニズムによる故障検出率を算出しています。
例えば、「要求なしでデータ転送される」ケースにおいては、
＜前回のメッセージの場合＞
E2E プロテクションによる検出率：100%（E2E プロテクションのメッセージカウンタまたはメッセージ ID から検出される）
＜ランダムな値の場合＞
E2E プロテクションによってエラー検出できない確率
・偶然に正当な CRC 値に一致する確率：0.39%（1/256）
・偶然に正当な ID に一致する確率：75%（12/16）
・正しいカウンタ値に偶然に適合する確率：6.25%（1/16）
⇒ エラーが検出できない全体の確率：0.39% × 75% × 6.25% ＝ 0.02%
E2E プロテクションによる検出率：99.98%（1-エラー検出できない確率）
２つの故障モードの配分の見積もりは省略し、ここでのダイアグカバレッジは 99.98%と見積もられています。
このように厳しめな近似として、２つのダイアグカバレッジのうち、より低い検出率を保守的に採用するといったアプローチも規格では許容されています。

**論理的根拠を“見える化”し、組織のナレッジに**

上記でご説明した通り、ダイアグカバレッジの見積もりは、単に計算する作業ではなく、ユースケースの具体化、故障モードの網羅、安全機構との対応付け、そして定量的な裏付けという一連の思考プロセスを通じて、安全性の論理的根拠を “見える化” する作業です。
この “見える化” によって、関係者間での共通理解が深まり、技術的な合意形成がスムーズになります。
ISO 26262 Part 11 Annex A の DMA 事例は、このプロセスを実践的に示したガイドと言えます。

プロジェクトに適用する際は、以下の手順となります。

1. 対象機能のユースケースとセーフティメカニズムを整理
2. 故障モードを網羅的に洗い出す
3. セーフティメカニズムごとに検出可能範囲を整理
4. 最も低い検出率を保守的に採用し、テスト・解析・シミュレーションで妥当性を積み上げる

こうして得られた評価は、“論理的根拠” を “見える化” した信頼性の高いダイアグカバレッジの見積もりであり、ISO 26262 における安全性の確保において極めて重要な役割を果たします。
なお、開発プロジェクトで実装するセーフティメカニズムごとに定量的評価を実施することは負担が大きいため、セーフティメカニズムと合わせて定量的評価結果を組織のナレッジとして蓄積し、開発現場における負担を軽減することも重要です。

現在、弊社では機能安全に関する新たなワークショッププログラムを企画中です。
今回ご紹介したダイアグカバレッジの見積もりやセーフティメカニズムの有効性評価は、PMHF（確率的ハードウェア故障指標）や EEC（各故障原因の評価）といった安全メトリックを正確に算出するための前提となる重要なプロセスであり、今後のワークショップで体系的に取り上げる予定です。

なお、これらの応用的な内容を理解するための前提として、6 月 27 日開催予定の「基礎故障率の算出とメトリック評価」ワークショップでは、IEC 61709 や SN 29500 に基づく故障率の算出方法や、PMHF・EEC の基本的な知識を演習や議論を通じて体系的に獲得いただけます。ダイアグカバレッジの評価結果を安全メトリックに正しく反映させるための基礎知識獲得の場として、ぜひご活用ください。

【関連トピックおよびワークショップ】
1)IEC61709 および SN29500 に基づく部品故障率計算における課題
https://biz3.co.jp/download/6889

2)機能安全実装ワークショップ ～基礎故障率の算出とメトリック評価～（6/27 開催）
https://biz3.co.jp/publictraining/7443

2025/5/22 大塚 愁