3章　効率的な設計開発の管理

ここでは，前章での検討を踏まえ，ロボットの開発工程として，先に触れた「リスクアセスメント」と「ソフトウェア開発」に着目し，これらの効率的な管理について，その取組み方の一端を検討する。

リスクアセスメントの取組みについて

リスクアセスメントでは，前提となる「ロボットの意図する使用を明確にすること」が必要である。誰が，いつ，どこで，何のために，どのように使うのかを明らかにすることによって，対象とするロボットの具体的な危険源の同定が可能となるためである。この活動で，開発するロボットに想定される危険源の同定を漏らしてしまうと，できあがったロボットが，ある危険源には対応できない未熟なロボットとなる可能性が否定できない。そのため，考えられる限りの危険源を同定することが重要である。

もし，対象とするロボットが，今までよりも高機能化や使用環境範囲が拡大した場合では，過去のリスクアセスメント結果を踏襲するだけではカバーできない可能性がある。そこで，リスクアセスメントの品質の観点として，たとえば，以下が挙げられる。

－網羅性
－整合性（一貫性）

網羅性については，まずはロボットの取りうる状態を漏らさず把握する。たとえば，アイドル状態，自動運転モード，手動運転モード，メンテナンスモードなどである。加えて，ロボットの周囲の環境が変わる場合も識別しておく。たとえば，「夜間は遠隔で運転状態の監視は続けられるが，周囲に人がいない」などである。次いで，各状態において想定しうる危険源を同定していく。その際，少なくとも一般的に考えられる危険源については，ひと通り想起することである。たとえば，ISO 10218–1（JIS B 8433–1）[8]の附属書 A で挙げられている危険源が参考になる。これに加えて，ロボット固有の危険源も同定する。今後，ロボットが，たとえばネットワークを経由してさまざまな機能が制御される場合には，これに応じた危険源の同定も必要となる。なお，ISO 10218–1（JIS B 8433–1）の附属書 A には，危険源の例として，その原因となる事象が約 80 件挙げられている。したがって，危険源の同定に関して検討されるシナリオ数が，少なくとも「ロボットの状態×80 件以上」想起されることになる。たとえば，ロボットが 4 状態あるとすれば，300 件以上のシナリオがリスクアセスメントシートに記載されることになる。

リスクアセスメントは，ロボットの使われ方やその振る舞いなどを前提としているため，設計の進捗によって，必要に応じて見直しが行われる。よって，改訂ごとに 300 件以上となるシナリオについて，保守やレビューを行って整合性を維持することは容易ではないと考えられる。管理された状態として，リスクアセスメントの結果を維持していくためには，現実的なシナリオ数に抑えておくことが肝要である。

そこで，網羅性と整合性を両立する方策を考察する。ここでは，重複する状況を集約し管理対象を合理化する方策として，下記に 2 段階のステップを示す。

－ステップ 1：ロボットの考え得る危険源と各状態をリストアップし，そのマトリクスを作成し，各危険源について，どの状態が該当するか分析し，検討対象とする状態を絞り込む（**図 8**）

－ステップ 2：ステップ 1 で絞り込んだ結果を踏まえて，リスクアセスメントを実施，以降，このリスクアセスメントシートをベースに保守を行う

もちろん，これらの記録類を証跡として管理することも忘れてはならない。

ソフトウェア開発の取組みについて

ここでは，通常のソフトウェア開発よりも厳格さが求められる安全関連制御システムのソフトウェア（以下，安全関連ソフトウェア）の開発に着目する。メーカーは安全関連制御システムを実現するためには，機能安全規格類に準じた開発を進める。機能安全の考え方は，**図 9** のように，ランダムハードウェア故障への対応とシステマティック故障への対応が求められる。なお，これらの用語の意味は，IEC 61508-4:2010（JIS C 0508-4:2012）[16]で次のように定義されている。

> 3.6.5　ランダムハードウェア故障
> 時間に関して無秩序に発生し，ハードウェアの多様な劣化メーカーニズムから生じる故障。
>
> 3.6.6　システマティック故障（決定論的原因

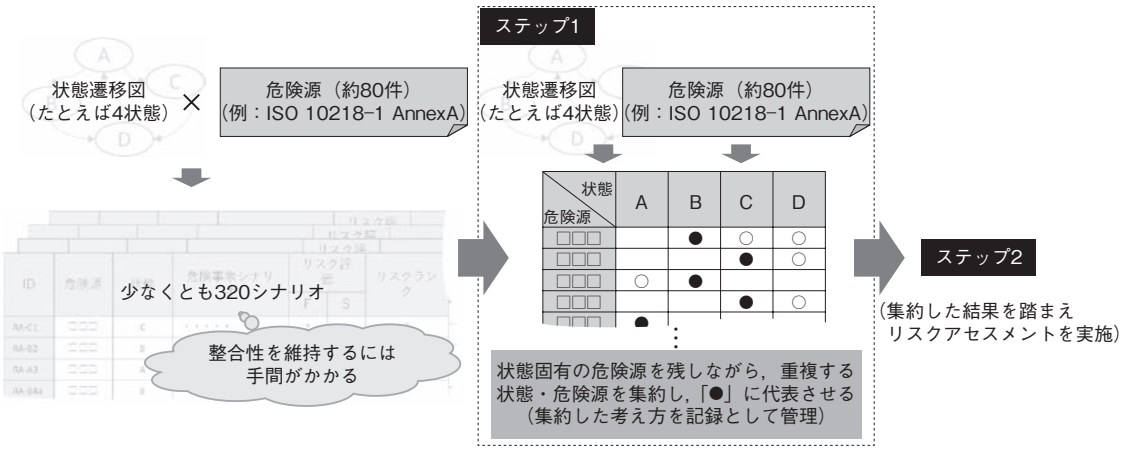

図8　リスクアセスメントで検討対象とする状態の絞り込みイメージ

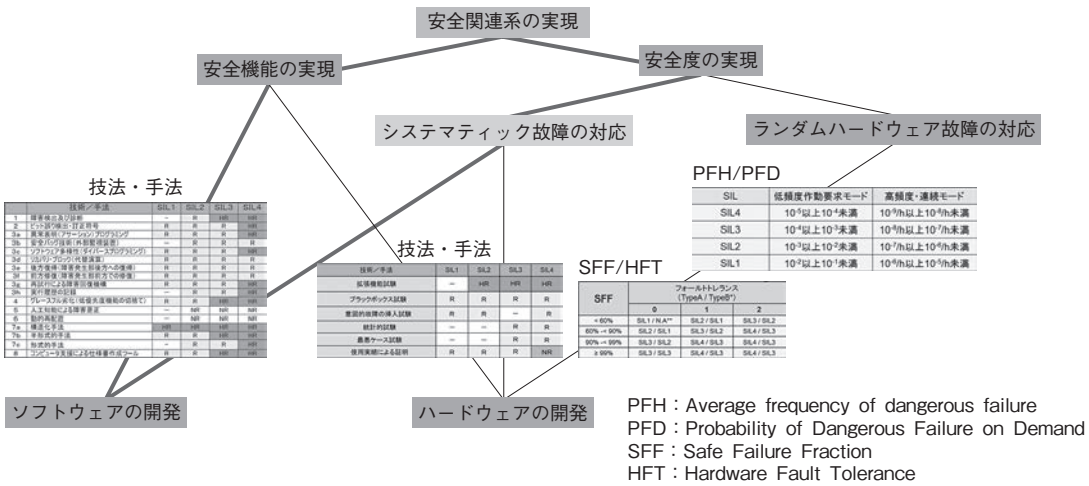

図9　機能安全の実現の考え方

表1　IEC 61508–3（JIS C 0508–3）における技法及び手段（抜粋）

開発フェーズ	主な技法及び手段
ソフトウェア 安全要求仕様	－準形式手法／形式手法 －前方／後方トレーサビリティ －コンピュータ支援仕様書作成ツール
ソフトウェア アーキテクチャ設計	－フォールト検出 －モジュラーアプローチ －前方／後方トレーサビリティ －構造化図表法 －コンピュータ支援仕様書作成ツール －最大周期を保証した周期的挙動 －最大応答時間を保証したイベント駆動
開発環境の指定	－適切なプログラミング言語 －認定したツール
ソフトウェア詳細設計 （モジュール設計及びコーディングを含む）	－構造化手法 －コンピュータ支援設計ツール －モジュラーアプローチ －設計及びコーディング基準 －構造化プログラミング －信頼性確認及び検証済みソフトウェア要素の利用 －前方トレーサビリティ
ソフトウェア モジュールテスト及び統合	－動的解析及びテスト －データの記録及び解析 －機能及びブラックボックステスト －テスト管理及び自動化ツール －前方トレーサビリティ
ハードウェア及びソフトウェア 統合	－機能及びブラックボックステスト －前方トレーサビリティ
ソフトウェア システム安全妥当性確認	－機能及びブラックボックステスト －前方／後方トレーサビリティ
ソフトウェア適合確認	－静的解析 －動的解析及びテスト －前方／後方トレーサビリティ

表2　オフライン支援ツールの分類[16),17)]

分類	説明	ツール例
T1	安全関連系の実行可能コードに寄与する出力を生成しない	－テキストエディタ －構成管理ツール
T2	ツール内にエラーがあっても欠陥をあきらかにすることはできないが，実行可能ソフトウェア内に直接エラーを生成することはなく，設計又は実行可能コードのテストまたは適合確認を支援する	－カバレッジ測定ツール －静的解析ツール
T3	安全関連系の実行可能コードに直接または間接的に寄与できる出力を生成する	－コンパイラ

故障）
正しい知識，認識，対策の欠如などの原因の決定的に関連する想定外の故障又は失敗。この原因は，設計の部分改修，製造過程，運転手順，文書化又はその他の関連する要因の修正によってだけ除くことができる。
（JIS C 0508–4：2012）[16)]

安全関連ソフトウェアは，安全機能の失敗確率を定量的に評価する方法が現時点では確立されていないため，システマティック故障への対応が必要である。その考え方は，ソフトウェア開発の各工程において，不具合を織り込まないことと，不具合があっても伝播を食い止めることである。そのために，たとえば，IEC 61508–3：2010（JIS C 0508–3：2014）[17)]では，要求される安全度のレベル（安全度水準）に応じて，**表1**のような技法の採用を求めている。詳細は，IEC 61508–3：2010（JIS C