ISO/TR 9839：ISO 26262-5 によるハードウェアへの予知保全の適用

CASE 領域の技術革新に伴い、より高い安全性が求められています。これに対応するため、ISO 26262 3rd edition への改定が検討されています。

その一環として、予知保全による機能失陥の未然防止や、人に依存しない劣化挙動の検出による適切なタイミングでのメンテナンスが必要とされ、2023 年 8 月に「ISO/TR 9839：ISO 26262-5 によるハードウェアへの予知保全の適用」が発行されました。ISO/TR 9839 の目的は、安全関連の E/E ハードウェアエレメントにおける劣化フォールトを検出するための予知保全方法の適用です。

ハードウェアエレメントは、時間の経過や摩耗によって劣化し、劣化の進行がハードウェアエレメントの故障を引き起こします。これを「劣化フォールト」といい、ISO/TR 9839 では、この劣化フォールトを検出し、意図機能が失われるまでの残存耐用年数を予測して適切な対応をとるための「予知保全」技術を考慮するためのアプローチが示されています。

これまでは、劣化フォールトは考慮されておらず、安全機構の実装による定量的評価指標の達成によって対処してきましたが、劣化フォールトに対する予知保全の適用が求められることになります。

本メルマガでは、予知保全の適用に向けて考えるべきポイントは何なのかを考えてみたいと思います。

劣化フォールト

特性は一定ではなく、時間とともに劣化し、劣化が限界閾値を超えて進行するとエラーや故障を引き起こす可能性があるフォールトを劣化フォールトと定義しています。

現在の ISO 26262-5 で考慮されているフォールト発生から機能不全に至るまでのライフサイクルモデルに、エレメントの劣化フォールトによるエレメントレベルのエラーや故障を考慮したライフサイクルモデルを図 1 に示します。

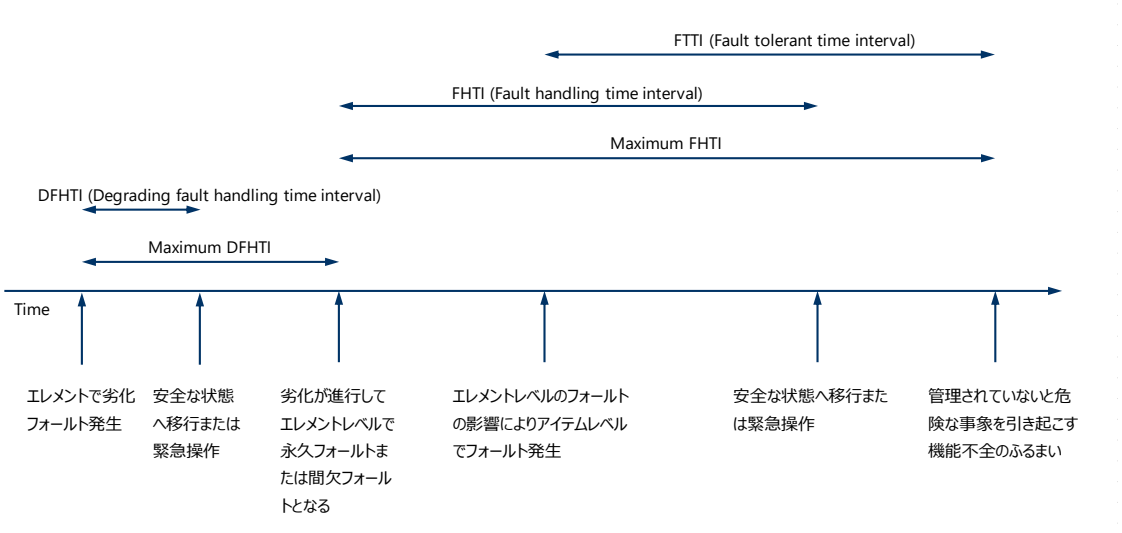

図 1. 劣化フォールトのライフサイクルモデル

劣化フォールトが発生してから、劣化が進行してエレメントレベルのエラーまたは故障を引き起こすまでの時間を最大劣化フォールトハンドリング時間間隔（DFHTI）と呼びます。これは劣化フォールトに対する予知保全のセーフティメカニズムの最大動作時間を示しています。フォールトハンドリング時間間隔（FHTI）と同様に、DFHTI は劣化フォールト検出時間間隔（DFDTI）と劣化フォールト反応時間間隔（DFRTI）に分けることができます。

残存耐用年数（RUL）

現在の時点から、任意のアイテムまたはエレメントが望ましい仕様内で意図された機能を果たさなくなると予想される時点までの期間を残存耐用年数と定義しています。

予知保全

劣化フォールトを検出し、意図機能が失われるまでの残存耐用年数を予測して適切に対応するために使用される技術を予知保全と定義しています。

予知保全技術によって残存耐用年数を見積もることができ、この結果によってエレメントがエラーや故障を引き起こす前に修理または交換することができるようになります。

ISO/TR 9839 では予知保全の具体的な技術手法に関しては記述されていませんが、劣化フォールトへのアプローチとして、劣化フォールトを検出し、残存耐用年数を予測するための予知保全のセーフティメカニズム実装例が示されています。

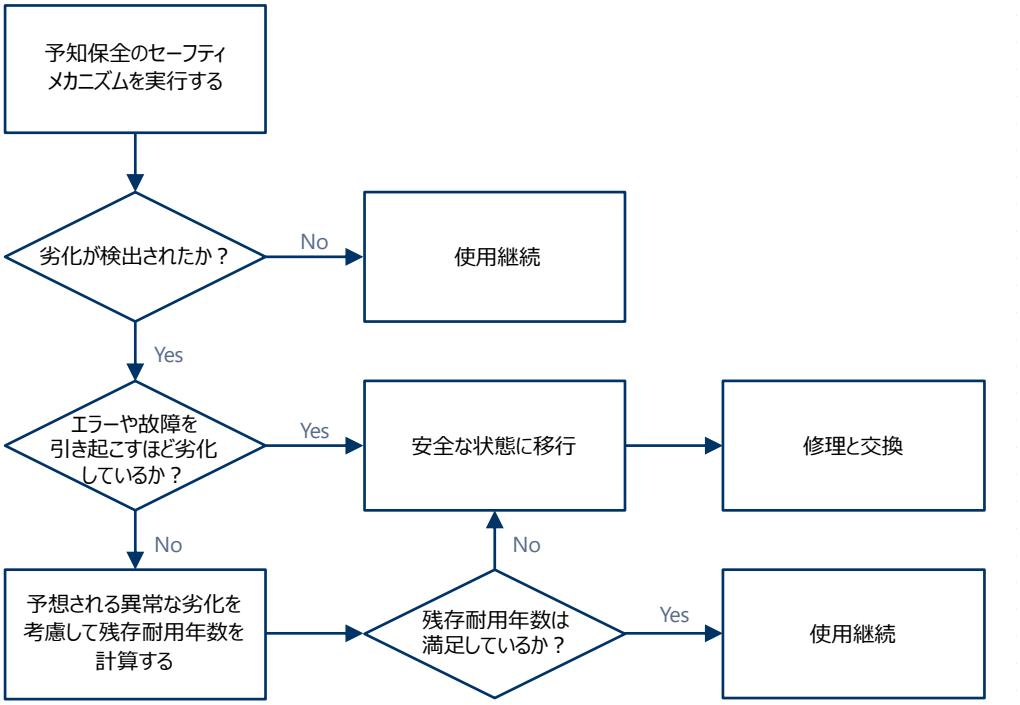

図.2 予知保全を検討するためのフローチャート

予知保全のセーフティメカニズムは、劣化フォールトに対するハンドリング時間間隔を満足する適切なタイミングと応答で定期的に実行する必要があります。図 2 に示すように、セーフティメカニズムを実行するたびに劣化のチェックを行い、劣化が検出されなければ、通常動作が継続され、劣化が検出された場合は処置が取られます。

劣化が進行し意図機能が失われる閾値を超えた場合は、劣化フォールトはエラーまたは故障を引き起こすため、劣化フォールト以外のフォールトと同様に危険な事象を回避するための安全状態へ移行され、修理または交換を受けて使用可能な状態に戻ります。

エラーや故障が発生するほど劣化が進行していない場合は残存耐用年数が計算され、駆動サイクルに十分な寿命が残っている場合は処置されず、通常動作を継続します。残りの寿命が駆動サイクルに対して十分でない場合は安全状態へ移行され、修理または交換を受けて使用可能な状態に戻ります。

現在、車両の平均使用年数は上昇を続けています。安全関連エレメントの本来の設計寿命を超えて運転されている可能性がありますが、予知保全によって危険事象を引き起こす前に劣化したエレメントを適切なタイミングで修理または交換することができ、安全な状態を保つことができます。

劣化の検出は、電気的な特性の変化や応答時間の変化をモニタリングし、ソフトウェアで劣化の度合いや進度を推測する仕組みが考えられますが、どの粒度で劣化を検出することが現実的なのか考える必要があります。

電子部品の劣化を検出しようと考えた場合、各電子部品に合わせた検出機構が多数必要となり、コストがかかり過ぎる上に、他の電子部品との相互作用によって検出できない可能性もあります。

機能単位で劣化の検出を考えた場合、いくつかの電子部品の劣化を包括的に検出できることになりますが、機能劣化の原因が複数考えられることにより、劣化の進度を予測することが難しくなります。

ISO/TR 9839 では予知保全の技術的な手法については触れられてはいません。そのため、ISO26262 3rd edition での予知保全の適用に向けて、各開発アイテム単位で劣化フォールトへのアプローチの適切な粒度を考えていくことが求められます。

弊社では、ISO 26262 の対応において、実装技術や手法に関するワークショップ、製品を開発していく中で直面する課題を解決する方法を議論するワークショップを提供しています。お客様と一緒に技術的な課題に取り組み、最適な解決策を見つけていきたいと考えております。ご興味がございましたら、お気軽にお問い合わせください。

今後も、ISO 26262 3rd edition への改定に関する最新の動向をお伝えしていきます。

2024/09/20 大塚 愁