

制御安全の国際規格 ISO13849-1 の改訂

制御安全に関する国際規格 ISO13849-1 の改訂版が 2015 年 12 月 15 日に発行された。従前より審議されていた ISO13849-1 と機能安全規格 IEC62061 の統合規格 ISO17305 は、2015 年 11 月 9 日に廃案となった。改訂内容の概要は下記のとおり。

(1) 要求パフォーマンスレベル PLr の決定

危険源への暴露の頻度及び／又は時間 F1/F2

- ・暴露頻度が 15 分に 1 回を超える場合で他に正当化を行えない場合は、F2 を選択する。
- ・累積された暴露時間が全体の動作時間の 1/20 を超えず、頻度が 15 分に 1 回以下の場合は、F1 を選択する事ができる。

改訂前は、1 時間に 1 回を超える場合は F2 となっていたので、条件が大幅に緩和された。

危険源回避又は危害の制限の可能性 P

- ・危険源回避又は危害の制限の可能性 P が危険源回避の可能性と危険事象発生確率の組合せとなり、危険事象の発生確率が低い事が正当化できる場合は、PLr を 1 段階低く見積もる事が可能。

(2) カテゴリ 2 に対する要求事項の変更

・改訂前は、指定アーキテクチャとしてのカテゴリ 2 に対してテスト頻度 $\geq 100 \times$ 安全要求頻度が要求されていたが、安全機能が要求されると、ただちにテストが行われ、機械を危険でない状態(通常は機械の停止)にするまでの合計時間が、危険源に到達するまでの時間より短くする事が可能であれば、テスト頻度の要求事項を満足する必要がない。

- ・PLr=a~c の安全機能に対してカテゴリ 2 を適用するには、安全状態を始動することが不可能である場合(例えば、最終開閉器における接点の溶着)、テスト装置の出力により危険を警告すれば実現可能。

以上により、カテゴリ 2 の適用可能性が広がった。

(3) 付属書 K 表 K.1 を用いた PL の見積(表 K.1 の拡張)

サブシステム毎にカテゴリ、平均危険側故障時間 $MTTF_D$ 、診断範囲 DC、共通原因故障 CCF に対する方策を見積もり、付属書 K 表 K.1 より危険側故障の発生確率 PFH_D を算出する場合、改訂前は $MTTF_D$ が 100 年に上限を設定されていたので、 PFH_D の値も 2.47×10^{-8} が上限となる。そのためサブシステムが 5 つ以上の安全関連部になると、下記のように PFH_D の値が PL=e の指定範囲を超えてしまい満足できなくなる。

安全関連部全体の $PFH_D = 5 \times 2.47 \times 10^{-8} = 1.23 \times 10^{-7} > 10^{-7}$

この問題を解消するために、表 K.1 の $MTTF_D$ の値が 2500 年まで拡張され、PLr の上限は 2.47×10^{-9} となった。

(4) 機械式、油圧式、空圧式もしくはそれらの混成からなるアクチュエータの PL

信頼性データがない機械、油圧、空圧(またはこれらの技術の混成または要素を含む)アクチュエータを出力として使用する場合、 $MTTF_D$ の値が算出できなくても、運用実績により証明されたデータなど一定の条件を満たせばカテゴリ、DC、CCF に対する方策から PL を算出する事が可能となった。

(5) その他の追加、変更点

- ・PL を見積もる際のパラメータにシステマチック故障に対する方策が追加。
 - ・定義に運用実績による証明、高頻度作動要求又は連続モードが追加。
 - ・一定の要件を満たせば、安全関連組込みソフトウェアの要求事項を満たしていない PLC を安全関連部に適用可能。
 - ・付属書 E.DC の見積の表 E.1 より出力装置の方策から E05 アクチュエータ監視なしの冗長化された遮断経路、E06 論理又は試験装置によるアクチュエータのうちの一つを監視する冗長化遮断経路が削除。
- など

今後の Schmersal Information で、(1)、(2)、(3)、(4)の内容詳細について個別に配信致します。

本件、お問合せは SCHMERSAL 日本支社迄。