

部 会 報 告

ISO/TC 127/SC 2/WG 24 (ISO 19014 土工機械—制御システムの安全) 2017年7月パリ国際作業グループ会議報告

標準部会 ISO/TC 127 土工機械委員会国際専門家 (Expert) 田中 昌也 (コマツ)

国際標準化機構 ISO の専門委員会 TC 127 (土工機械) 傘下の国際作業グループ ISO/TC 127/SC 2/WG 24 (ISO 19014 土工機械—制御システムの安全) 会議が 2017 年 7 月にフランス国パリ市で開催され、協会標準部会 ISO/TC 127 土工機械委員会から前回 6 月に引き続き国際専門家 (Expert) として出席した田中昌也氏の報告を紹介する。

会議：ISO/TC 127/SC 2/WG 24 国際作業グループ会議

1 開催日：平成 29 年 7 月 11 日 (火) ~ 13 日 (金)

2 開催地：フランス・パリ FICIME (Fédération des Entreprises Internationales de la Mécanique et de l'Electronique) 会議室

3 出席者：9 名 + Web 参加 2 名 (イタリア 1, ドイツ 1)

英国 Part 1 プロジェクトリーダー

米国 Part 2 プロジェクトリーダー 他 3 名

オーストラリア Part 5 プロジェクトリーダー

ドイツ 1 名

フランス 1 名

日本 1 名

4 議題

ISO 19014-2 (制御システムの実装と評価) の WD 作成。

- NWIP 時に添付したドラフトへのコメント審議
- コントローラハードウェアへの要求事項を Part 6 に分離するか Part 2 に含めるか。
- 油圧制御回路の記述内容 (オーストラリア専門家の提案文書 N 185 をレビュー)

ISO 13849 との関係について議論 (オーストラリア専門家の提案文書 N 180 をレビュー)

5 会議概要

- ・オーストラリア専門家の提案文書 N 180 をレビュー

N 180 は、「建機をはじめとする mobile machinery への適用を考えた場合、ISO 13849 にはやや不明確な部分があり (B 規格なので当然ではあるが)、それ故 ISO 19014 (C 規格) を作成する必要がある」という

white paper。いったん WG 24 から SC 2 に提出されていたが、WG 24 に差し戻されてきたので WG 24 メンバーはコメント提出、9 月の会議でレビューした上で WG 24 内で投票し、結果を SC 2 または TC 127 へ送付する。

- ・NWIP 時コメントの審議
- ・新ドラフト (N 182) のレビュー
議論の結果を織り込んだテキストを作成 (米国宿題)
- ・オーストラリア専門家の提案文書 N 185 をレビュー

N 185 は油圧制御系で MPLa=d や e が構成できることを説明する技術論の案。5 つの案 (どれも完璧ではない) が示されているので、好ましい案を回答または代案を出すこと。その後、11 月の会議で回答結果を審議してドラフトに反映する。今回のレビュー結果を織り込んだ改訂版を作成 (オーストラリア宿題)

6 会議メモ

ベースとなる規格 (ISO 13849, IEC 61508) との関係について

安全関連制御系の達成度合い (MPLa) を評価する部分 (耐環境性要求事項以外) のベースは ISO 13849 と IEC 61508 である。元々は ISO 19014 だけで完結するように必要部分は全て引用してくる計画だったが、IEC から引用の許諾が下りないことや、ほとんど引用なら元規格との差分が解ったほうがよい、ということで、同一内容については元規格を参照とすることとなった。これに伴い、コントローラハードウェアへの要求事項は Part 2 に含める (IEC 61508 への参照項目が大半と予想されるので) ことに決定した。

ソフトウェアに対する要求事項は ISO 19014-4 独自の内容となっているので、このまま進める。

スコープについて

ISO 19014 の対象に含むかどうかでもめていたものが、再度俎上にのぼり議論された。

- 1) immediate action warning system, collision avoidance system

たびたび話題になり結果が二転三転しているが、や

はり機械の動きにかかわらないものは ISO 19014 のスコープ外、というのが優勢。但し英国専門家から「MPLr を割り当てないにしても、immediate action warning system の信頼性（或いは Safety integrity と言うべきか）に対して業界の見解を示すべきである」との意見あり。Collision avoidance system については、制御（ブレーキをかけるなど）に使う場合は ISO 19014 適用となることには、反対意見無し。

2) fire suppression system

Hazardous Situation が起こらないようにするのが Functional Safety であり、Hazardous Situation（この場合車両火災）が起きてしまった後に働くものは Functional Safety ではないという理由で除外。

Fault Exclusion

オーストラリア専門家が認証機関に聞いた意見として「Fault exclusion とは $MTTFd = \infty$, $DC = HIGH$ と考えられる（として計算に含めると深読みできる）」

というのを紹介したが、ISO 13849 には「Fault exclusion は $MTTFd$ や DC の計算から除くように書かれている」のが会議参加者の共通認識であり、議論の結果、以下の文書となった。

1. fault by fault basis - after all fault are identified some faults may be fault excluded.
Others could be handled by diagnostic means within the control system.
2. system component level - if all known faults can be fault excluded within a system or at the component level, then system or component can be fault excluded entirely it then is not included in the calculation nor can a performance level be claimed.

以上

