

部 会 報 告

ISO/TC 127 (土工機械) 2014 年 6 月 スウェーデン王国ストックホルム市での国際作業グループの会議報告 ISO/TC 127/SC 2/WG 24 (ISO 19014 制御システムの安全) 会議 ISO/TC 127/SC 3/WG 9 (ISO 14490 規格群 電機駆動式機械並びに 関連構成部品及び装置の電気安全) 会議

標準部会 ISO/TC 127 土工機械委員会国際専門家 (Expert)

田中 昌也, 尾畑 功治 (コマツ)

2014 年 6 月 23 日～の週に国際標準化機構 ISO/TC 127 (土工機械専門委員会) の国際作業グループなどの会議がスウェーデン王国ストックホルム市の SIS スウェーデン規格協会で開催され、協会標準部会 ISO/TC 127 土工機械委員会から国際専門家 (Expert) として出席の田中氏及び尾畑氏の報告を紹介する。

1. ISO/TC 127/SC 2/WG 24 (ISO 19014 制御システムの安全) 国際作業グループ会議

1.1 開催日：2014 年 6 月 23 日～25 日

1.2 開催地：前記スウェーデン王国ストックホルム市 SIS スウェーデン規格協会

1.3 出席者 (敬称略)：オーストラリア (SA) 1 名：Alex Watson (Caterpillar), チェコ (UNMZ) 1 名：Pavel Urban, Doosan (斗山/Bobcat), ドイツ (DIN) 1 名：Frederic Knecht (Liebherr), イタリア (UNI) 4 名：Giorgio Garofani 氏, Paolo Ferracin 氏, Francesco De Rosa 氏 (CNH), 他に 1 名氏名所属不詳, 日本 (JISC) 1 名：田中昌也氏 (コマツ), スウェーデン (SIS) 2 名：Richard Hendeberg 氏 (Atlas Copco Rock Drills), Mats Karlsson 氏 (Volvo Construction), 米国 (ANSI) 5 名：Dan Roley 博士, Jeff Carter 氏 (Caterpillar), Rick Weires 氏, Michael D. Peat (John Deere), Steve Neva 氏 (斗山/Bobcat), 英国 (BSI) 2 名：Victoria Huston 氏 (JCB), Philip Webb 氏 (英国コマツ), 計 17 名

・コンビナー (ISO の国際作業グループ主査のこと)
前記 Dan Roley 氏

・Part 1 プロジェクトリーダー (以下 PL と略す)：前記 Victoria Huston 氏

・Part 2 及び Part 3PL：前記 Rick Weires 氏

1.4 経緯及び概要：

◆審議規格案

- ISO 19014-1: Earth-moving machinery -Safety-Part 1: Risk assessment methodology to determine control system performance requirements 土工機械—安全—第 1 部：制御系の性能要求事項を決定するためのリスクアセスメント手法
- ISO 19014-2: Earth-moving machinery -Safety-Part 2: Design and Evaluation of Safety-Related Electronic Machine Control Systems 土工機械—安全—第 2 部：安全関連電子式機械制御系の設計及び評価
- ISO 19014-3: Earth-moving machinery -Safety-Part 3: Environmental Testing 土工機械—安全—第 3 部：環境試験

◆経緯：建機の機能安全規格として 2008 年に ISO 15998-1 が制定済みで、その適用ガイドライン ISO/TS 15998-2 が 2012 年に制定された。しかし多大な苦労を重ねて作成した ISO/TS 15998-2 をもってしてもリスクアセスメントを「だれが何度やっても同じ結果になる」は達成できておらず、早々に改定提案が出された。その 3 回目。今回より 3 つのパートに分けて審議される。

◆公式議事録：発行済 (ISO TC127 SC2 WG24 N37)

1.5 決定事項：

- ◆7/31 までに次回案文に織り込みたい項目を送付する。(全員)
- ◆8/25 までに次回案文を用意する。(Huston 氏, Weires 氏)
- ◆10/31 までに 8/25 版の案文に対するコメント送付。(全員)

1.6 宿題事項：個別の宿題として

(1) SIL/PL のバリエーションすなわち SIL (IEC 61508, IEC 62061, ISO 15998?), PL (ISO 13849), AgPL (ISO 25119), ASIL (ISO 26262) の横にらみを 10/24 まで。スウェーデン宿題。

(2) データコネクション (通信) への要求事項のたたき台。イタリア宿題。

ISO 15998-1 AnnexD を出発点にして、将来の技術も考慮する (車車間通信のような、車両の外部との通信)

(3) Part2 ドラフトに対する油圧・メカ制御システムの差分。オーストラリア宿題。

1.7 次回会議予定：11/12～14 (14のみ未確定) フランクフルト

1.8 所見：

(1) プロジェクト進捗：前回までは案文もなく方向性が見えなかったが、今回は Part1 については事前に案文が配布され、Part2 についても会議直前に案文が配布されて席上概要説明があったため議論は白熱したものの争点はある程度見えてきた。今後の意見提出・会議発言は重要。

(2) 豪州での IEC 61508 要求について：建機や自動車、農機のような組み込み制御系では機能安全の規格として IEC 61508 (B 規格) をそのまま適用するのは無理があるとして、それぞれの業界の C 規格を制定している。ISO 19014 のこれまでの議論でも IEC 61508 を積極的に推す人はいなかったのだが今回豪州代表 (Watson 氏) が豪州の州政府 (全ての州ではないらしいが) が IEC 61508 を要求しているので ISO 19014 を IEC 61508 と整合させるよう強く主張していた。

=====

(議事メモ)

Part1

・PLr を求める部分。JCB 社の Huston 氏が引き続き担当

* PL: Performance Level, SIL のような尺度。プロジェクトリーダーと同じアクリロニムだが文脈で判別してください。

・車体全体のリスクアセス手順 (ISO12100) と MCS (Machine Control System) のリスクアセス手順 (ISO19014) のつながり・分担 (ハザード抽出) で議論になった。決着せず。

・S (人的被害の大きさ), F (リスクにさらされる頻度), P (リスクを回避できる度合い) から PLr を

求める方法について。

ISO 25119 方式か数値的方法 (スコアを計算する方法) のどちらかにする。

要点は S が大きくても他のパラメータ次第で低い PL になりうる方法であるということである。これは ISO 15998 でこれまで例示されてきたリスクグラフと大きく異なる (これらでは人的被害が大きいと高い PLr/SIL に固定される)。

冒頭に記述したように Watson 氏から IEC 61508 より甘くなるのは問題との発言あり。

・上のトピックに関連した議論として、人的被害として人数を考慮するかどうか。

Part2

・制御系を実装して PL を評価する部分。

ISO/TS15998-2 を担当した Weires 氏が PL であるが同じ John Deere 社の Michael Peat 氏が案文を執筆した模様。

Peat 氏がパワーポイントの資料で概要を説明 (この資料は配布されなかった)。

・ISO19014 のスコープには電気・電子制御システムだけでなく油圧・メカによる制御システムを含むことになっているが、今回の Part2 のドラフトは電気・電子制御システムだけを対象とした。

・「MTTFd の Target を要求しない。理由はワイヤハーネスの故障率が大きいのにそれを求めるのが難しいので MTTFd が正しく計算できないから。かわりに HFT (Hardware Fault Tolerance) と SFF (Safe Error Fraction) で評価する」と提案があったがちょっと大胆すぎる。そもそも SFF を計算するのにもハーネスの故障率は必要ではないか? 会議でも同趣旨の疑問がイタリア代表から提示された。

議論になるも決着せず。

・PL は 13849 の PL をそのまま使うか? それともモディファイするか? (ISO25119 の AgPL のように) との議論あり。結論出ず。サブシステムを他社から購入する場合 ISO19014 で作ってくれというのはムリがあるのでサブシステムは ISO26262 などを認めることにしてはどうかという流れになって、では換算表が必要になるのでまずは横にらみをしようということになった (ASIL, AgPL, SIL, PL...)。

・Warning device に PLr を割り当てるか?

オペレータに安全上重要な情報を提示する Warning device はきちんとつくらないといけないと考える (このこと自体は正しいが) 人が PL を割り当てるべきという主張をするようによく議論になる。言い

たいことはわかるのだが、ISO15998-1/2 制定時に決めた SCOPE は尊重されるべきという指摘あり。ロックドリルの規格（番号不明）ではインジケータにも PL を割りあてているそうである。

また Safety Function が一部失われている状態（二重系の片方が死んでいる状態など）はオペに通知する必要があると考える人もいる。

（以下考察）

IEC61508 には高頻度モードと低頻度モードが定義されている。100Hz で動いているような制御ループは高頻度モードで、自己診断で異常を検出したら安全状態への移行は自動で行われる必要がありオペレータによる処置は期待できない。ISO15998 では高頻度モードかつハザードを「機械の異常な動き」を前提にしているので警告表示ししかないものはスコープ外になっている。ISO13849 ではおそらく低頻度モードと高頻度モードを層別していないので自己診断による警告表示+オペレータの介入という設計も包含されている。Safety Function に要求される応答時間をどこで区切るかという問題が一つと検討すべきハザードを拡張するか（感電なども扱うか）だと思う。

- ・全体的に ISO25119（農機の機能安全）の内容がかなり流用されている。

内容をよく見て不都合のあるところはコメントを出して修正を要求する必要あり。

- ・前回会議で「ソフトの実装について、V 字プロセスに限定されないようにしよう」という提案が Weires 氏からあった。アジャイルやインクリメンタル開発とった new technology を取り込むべき、というのが今回その説明はなく、ドラフトにも見当たらないように思われる。

Part3

- ・耐環境試験。Part2 と同じく Weires 氏が PL。
- ・IEC に揃えようという提案。

以上

2. ISO/TC 127/SC 3/WG 9 (ISO 14490 規格群 電機駆動式機械並びに関連構成部品及び装置の電気安全) 国際作業グループ会議

2.1 開催日：2014 年 6 月 26 日, 27 日

2.2 開催地：前記スウェーデン王国ストックホルム市 SIS スウェーデン規格協会

2.3 出席者（敬称略）：ドイツ（DIN）3 名：Oliver Fenker (Liebherr) 氏, Jochen Hovelmann 氏 (KMG),

西畑孝志氏（従来日本のコマツから参加、今回は KMG から参加）、日本（JISC）2 名：田中昌也氏、尾畑功治氏（コマツ）、スウェーデン（SIS）1 名：Stefan A. Nilsson 氏（Volvo Construction）、米国（ANSI）4 名：Dan Roley 博士（Caterpillar）、Rick Weires 氏、Gary Weidneer 氏、Orrin West 氏（John Deere）、他に電話（ウェブ）参加者 2 名、計 12 名

・コンビナー（ISO の国際作業グループ主査のこと）
兼 PL：前記 Rick Weires 氏

2.4 経緯：

◆**審議規格案**：ISO 14990 Earth-moving machinery - Electrical safety of machines utilizing electric drives and related components and systems 土工機械—電機駆動式機械並びに関連構成部品及び装置の電気安全

－ Part1: General requirements 第 1 部：一般要求事項

－ Part2: Particular requirements for externally-powered machines 第 2 部：外部電源機械の特定要求事項

－ Part3: Particular requirements for self-powered machines 第 3 部：電源搭載機械の特定要求事項

◆**経緯**：交流 50 V-36 kV, 直流 75 V-36 kV のオンボード電圧を利用する土工機械の電気安全規格として ISO 14990 を策定中。IEC 60204-1 をベースに原案を作成してきた。途中 IEC/ISO 間の著作権問題などがあったが WD を基に 2013/9/25 に CD（委員会原案）発行。投票の結果、賛成多数で文書は承認されたが、SE, US, DE から多数の修正提案が提出された。この修正提案の審議のため WG9 会議が開催された。

◆**公式議事録**：回覧待ち

2.5 出席の目的／活動方針：

- ・電動化が進む土工機械で電気安全問題が生じないように、国際標準を策定する。
- ・最新の原案審議情報を入手し内容を確認。必要に応じて修正意見を提案することで、土工機械の電気安全に関する技術の国際標準化をサポートする。
- ・この際、電動化が進む日本メーカの知見を原案に反映することで、国際標準の適正化をサポートする。

2.6 結果：

(1) CD 文書に対する各国コメントと修正提案が逐次審議された。

(各国コメント -1：139 件, -2：10 件, -3：13 件)

(2) 日本は事前に -1 に対し、コンボ単体に加えてコ

ンポ組合せ状態での耐電圧試験に関する修正提案 2 件、-3 に対し、ISO 6469 に基づく設計を許容する修正提案 1 件提出。

(3) しかし、-1 では耐電圧試験の繰り返しが絶縁に及ぼす悪影響は認めるが、組合せ試験は必須。-3 では IEC 60204-1 に従属する方針に反するとのことで他委員の賛同を得られなかった。

(4) 特に、システム組み合わせ状態での耐電圧試験の規定では US 提案と衝突し、2 時間近くの議論になった末、US 提案（試験実施）が採用された。

(5) 最終的に必要なのは製品の電気安全であり、これを担保する方法は必ずしも耐電圧試験だけではないと考えられる。国内メーカの意見を聞いて再提案を検討する必要がある。

(6) 他国の主だった技術提案は、

- ・アルミニウム電線サイズ規定 ($\geq 16 \text{ mm}^2$): [accept]
 - ・電池メーカ推奨仕様の厳守: [not accept]
 - ・ケーブルの耐電圧試験電圧規定 ($\geq 2000 \text{ V}$, 5 min): [accept]
 - ・システム組み合わせ状態での耐電圧試験の実施: [accept]
 - ・DC での耐電圧試験の許容: [accept]
 - ・モータ端子箱絶縁構造の規定追加（絶縁隔壁／絶縁空間）: [accept]
 - ・異常時の警報／保護システムの規定追加: [accept]
 - ・銘板記載事項の追加: [not accept]
 - ・教育／サービスマニュアルの充実: [accept]
- 等。IEC 60204-1 との整合性で逸脱しない提案は概ね認可となった。

(7) 新しい点では、充電式土工機械も ISO 14990 でカバーすることとなり、充電状態は -2, 非充電時は -3 で電気安全性を規定することとし原案を修正することになった。

2.7 問題点：日本の修正提案 3 件には賛同が得られないまま、CD → DIS に移行。

2.8 今後の予定：

- ・9/1 までに会議結果を受けたドラフトを用意し、WG に配布（Wires 氏、Weidner 氏）。
- ・WG 内に配布後、3 週間で WG メンバレビュー（全員）。
- ・12/1 までに幹事国（日本）に DIS 送付（Wires 氏、Weidner 氏）。
- ・投票 3 ～ 6 ヶ月（投票完了）
- ・投票結果および各国コメントを精査して、会議招集／非招集で FDIS に移行するか決定。

2.9 次回会議時期：2015 年中旬（必要時）。

2.10 協会及び委員各位への依頼：

- ・次回案文（DIS）で修正すべき点が無いか確認（特に今回賛同が得られなかった日本コメント関係部分）
- ・各社意見収集
- ・必要に応じて WG9 会議参加（特に技術意見提出時）

J C M A