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）2016 年 11 月～ 12 月 米国ドラル 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）内の特設グループ会議が 2016 年 11 月～ 12 月にかけて米国フロリダ州マイアミ近郊ドラル市で開催され，協会標準部会 ISO/TC 127 土工機械委員会から前回 8 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 国際作業グループ内 Ad Hoc Group（特設グループ）会議

1　**開催日**：平成 28 年 11 月 29 日（火）～ 12 月 2 日（金）

2　**開催地**：米国フロリダ州ドラル市　JohnDeere 社会議室

3　**出席者**：13 名

米国　Part 2 プロジェクトリーダ，Part 3 プロジェクトリーダ，他 5 名

英国　Part 1 プロジェクトリーダ，他 1 名

イタリア　Part 4 プロジェクトリーダ

オーストラリア　Part 5 プロジェクトリーダ

スウェーデン　1 名

日本　1 名

公式議事録：ISO/TC127/SC2/WG24/Doc N148 参照

4　会議概要

Part 1（MPLr の割り当て）：ドラフトを修正し再投票（2nd DIS）を目指す。

DIS 投票結果は否決だったが，コメントの審議を行いドラフトの修正を行った（但し途中まで）。2017 年 1 月に会議を開催し，引き続きコメント審議を行う。プロジェクトリーダは，ここまでの清書版案文を作成し，次回の WG 会議前に配布する。

Part 2（制御システムの実装と評価）：時間切れのため，下記の進め方とする。

1）規格作成期限が迫っており，（自動キャンセル回避の為）プロジェクトの自発的取り下げを行うが，案文作成の実務は継続する。プロジェクトリーダは，今回会議の結果までを織り込んだ清書版案文を作成し，配布する（2017 年 1 月）。CD 投票に耐えるレベルの案文が完成した時点で，ISO 管理上のプロジェクトを再開する。

2）ソフトウェアへの詳細要求事項が Part 4 としてすでに分離されているが，さらに，コントローラの回路設計への詳細要求事項を Part 6 として分離することが決定した。米国から新たなプロジェクトリーダを任命する予定。目論見通り ISO 19014 Part 2，Part 4，Part 6 が完成した暁には，建設機械の制御系設計において IEC 61508 への参照は不要になる筈である。

Part 3（耐環境性要求事項）：FDIS 投票に進む。

日本コメントはほぼ受け入れられたが，振動試験を正弦波形のみとすることは認められなかった。また，Operating Shock（5.7）と Thermal Shock（5.10）の動作ステータスをクラス A からクラス C に修正すべきという意見は認められなかった。Chemical Resistance（5.3），Salt Spray（5.4）については認められた。

Part 4（ソフトウェアへの要求事項）：CD 投票に進む。投票期間は 12 週間。

現状文書で CD 投票にかける。追加の意見があればコメント提出すること。

5　日本のアクション

Part 1，Part 5

Part 1 の内容を試行して Part 5 を作成し，その結果を Part 1 にフィードバックすべきと思うが，まず Part 1 を決めてしまい，その後で Part 5 を作ればよい，という考えで進めようとしているように感じられる。試行例をできるだけ集めて問題点を指摘すべき（可能なら代案を提出すべき）と考える。

Part 2，Part 6

電気を使用しない制御システムについてどのように記述すべきか，日本案（案文）を WG に提案したい。電気電子制御システムについても，ベースとなる ISO 13849 であまり説明されていない部分の記述を決めていく必要がある。（詳細な要求をしないならしない，要求するならどういう要求事項にするか。電気電子制御システムのカテゴリ 2 の解釈，CPU を well-tried として扱うか否か，等）

Part 3

概ね懸念は解消された。但し，ISO 15998-1 の環境試験の項目を参照している規格は，今後，ISO 19014-3 を参照することになると思われ，コントローラ以外の車載電子機器は注意が必要と考える（メーカの判断により独自の試験水準を設定できる余地が少なくなっている）。

Part 4

バス通信に対して過大な要求にならないようにする。

6 議事メモ

重要なコメントの審議結果を報告する。

Part 1（ドラフト：N 0144 コメントシート：N 0143）

*行先頭の符号（DE003 や UK007 等）は，コメントシートの通し番号を示す。US コメントのみ，US コメントの通し番号と全体の通し番号が振られている（例：US001/002）。

US001/002 3.3.1 MCS
MCS と safety related machine control system［SRP/CS 3.3.2］の関係は？
safety related でない control system は，scope に入るか，入らないか？
この点は，いつまでたってもクリアにならない。
MCS と SRP/CS を分けると，Part 2 が煩雑になる。
EMCS にも MCS と SRP/CS
NEMCS にも MCS と SRP/CS が必要になる
Part 2 の N 136 の Figure 4 で表現するのがよい。
この図を正しく描くべき。
MCS - SCS - SRP/CS という階層構造
SCS 安全関連制御システム：MCS のうちで安全に関係するもの，という定義を導入する
EMCS -> MSCS
NEMCS -> NESCS
functional safety との関係は？
safety function
この辺りの基本的な定義を各 Part 間で整合させる必要がある。
3.3.1 は，まだ矛盾している感がある。
危険な故障モードがあるのが SCS というのは理解できる。
しかし，それと SCS が同じ定義であるのは疑問。
UK007
最新の proposal が添付されていない（前回の Ad Hoc 会議の結果が添付される筈だった）。
US079/166
exposure の提案がエクセルで埋め込まれている。
Use case の最悪値を選ぶので，合計は 100% にならない。→それで良いのか？
Abuse は除いてよい。
正確なパーセンテージは計測できないので，subjective に数字を入れる
E は A，H，P から計算する。詳細は Annex D に記載
Use case の計算について議論
平均値では，うまく説明できない（オーストラリア専門家意見）。
・repeatable across the industry
・ISO 12100 の intended use を説明できることが必要。
Use case に Variety がある場合は，use case を代表できない
これらが満たされれば平均でもよい。
複数ある use case から，比率の最大の分類を選ぶ
population のデータを得るのは困難といった説明をうけたがどうもしっくりこない。
SE030
ISO 26262 全体を参照することはしない。必要な項目をコメントとして提出のこと。
→スウェーデンの宿題
SE031
故障率がわかれば，ASIL と MPL を換算できるのでは？
→今のところ換算はできない。
もし可能であれば，電子機器を外部調達する際に便利ではある。
SE035
ワイパーは安全関連か？これを除外する定義を書く必要あり。
SE051
disagree
SE052-054
autonomous は ISO 17757 でカバーする。
US020/075
WG agree
warning device に PL を割り当てるのか？
ISO 16001 からの参照　環境試験 ISO 15998 or ISO 19014
integrity として ISO 19014 を要求している規格もある？
MPLr をつけるか？　→ Part 5 で検討する。
US025/081,028/085
オーストラリア提案に基づき definition を変更する。
application：建設機械ユーザが供用する産業。鉱山，道路工事など。

US089
MCSSA ISO 12100 のリスクアセスメント（車体全体のリスクアセスメント）プロセスと安全関連制御システム（SCS）のリスクアセスメントプロセスを混同しないように用語を定義する。
PHA? というアクロニムもあるが, これは却下された。
SCS に MPLr を割り当てるプロセスを指す。
スウェーデンは，公道上での使用を随分と気にしていた。
以下　terms and definition が続く
hazard zone：コントローラの故障による影響範囲とする。
12100 の定義（一般的な hazard zone）から変更する
US041/101
規格本文には要求を書くべきであり，要求ではない文書を延々と書くべきでない。
（Note に記載すべき）
SE103,104
disagree
US046/111
4.1 回路自体に感電することはスコープ外とする。
IT144
warning device に何を要求するか？　→　Part 2 で触れるべき。
US065/148
agree delete 5.3
6.1 Part 1（MCSSA）では詳細設計を考慮しない。これを英語でどう表記するか。
また，シートベルトは MPLr の外のものである。→どう文書化するか？
US075/162
此処までで時間切れ。
被害度（severity）は，最悪値ではなく，最も起こりうるものをとる，筈だったが，また最悪値に戻そうとしている。この点を指摘したが，ISO 19014 を成立させるにはドイツや CEN（欧州標準化委員会）の理解を得ることが必須であり止むを得ない，とのことである。それはわかるが，必要以上に厳しくすると現実離れした結果（全部 MPLr=e）になってしまうと思うので，現時点では反対という意思表明をした。
オーストラリアが，ISO 13849 が建設機械に適用する場合課題があり，ISO 19014 を新しくつくる理由を書いた論文を配布する。

Part 2（ドラフト N0136，コメントシート N0135）

＊Part 2 のコメントシートには通し番号が振られていないため，次のように表記する。
AAB-C：AA（国）B（コメントシートのページ）C（各ページにおける国別コメント順序）
JP1-1，US3-1
電気電子を使わない制御システムの記述について。
Alton（Peoria?）で議論した結果がドラフト（N136）に反映されている。
カテゴリ等の概念は維持するが，解釈が異なる，ということらしい。
メカ制御系の規格として ISO 4413 はどうか？→ ISO 4413 は機能安全の規格ではない。
US2-3 introduction
ISO 26262 は次の改訂（2019）で全ての公道走行機械を含めようとしているようだが，ISO 26262 は土工機械を規定できない。（TC が異なる）
US4-1，4-2 FPGA,ASIC
IEC 61508-2 Annex E and F or ISO 26262-5 を参照する
参考　ISO/DIS 26262-11 で CPU を扱っている。
US6-1 audible warning
リスクアセスメントの結果により，オペレータの操作を期待してもよいことにする
しかし I-L-O の O ではない。TE の出力である。それでいいのか？
US7-2 Annex A から引用されているが，normative reference からは削除し Bibliography へ移動する
US9-1 3.11 EMCS 3.30 NEMCS
MCS は Part 1 に記載されている
IT10-5 agree
US13-8 Part 2 と Part 4 で整合させるべき
US15-2 E-stop（6.2.3）Estop が常に安全とは限らない。6.2.4 との違いは？
US15-8 agree
Part 2 には system integration と hardware が含まれており，混然としている
V モデルをどのように適用するか？
IT16-1 コメントはドラフトに織り込まれたと思われる
will be reviewed
US16-4 MPLr，MPLa という記号の使用に賛成。要求されるレベル，達成されたレベルに別の記号を割り当てておくことで，社内教育の際に理解されやすいとの意見があった。
US17-1 proposal DC
1）自分で FMEDA する
2）サプライヤから 1）相当を入手する
3）Annex D のテーブルを使用する

soft error? IEC 61508 を参照
DC（Diagnostic Coverage）は ISO 13849 に従うか IEC 61508 に従うか？
IEC 61508 では，全てのブロックが同じレベルの SFF でなければならない
ISO 13849 は平均でよい。（DC が低いブロックがあってもよい）
上記 2 点米国専門家の見解だが，要確認。
現時点では informative だが，normative にするか？
後で変更しやすいように informative にしておく。
ここまでで時間切れ。

Part 3（ドラフト N0146，コメントシート N0145）

*行先頭の符号（US1 や UK7 等）はコメントシートの通し番号

001EB（CEN コメント）
…2017 年 7 月にイタリアで会議を開催し，コメンター（EB）に直接説明する。
DE003 中身を読んだとは思えないコメント。
JP010 safety-related parts かどうかは ISO 19014-1 で決定する。
FR011 68 は IEC 60068 の誤記
US012 ISO 13766 をどう引用するか？
ISO/DIS 13766-1,2（＋バージョン？）とする。現時点では（新）ISO 13766 を引用することはできない。
SE016 ISO 26262 を直接引用していないので，ISO 26262 は参照しない。
US023 lifecycle とはどこからどこまでか。どの個体をとるか？平均？最悪値？車体の寿命？電子機器の寿命？→ lifecycle の定義は共通としておき，何の lifecycle かは各章で定義する。
IT032 ISO/DIS 13766 は ISO/DIS 13766-2 だけが参照される。
SE034 disagree。 example は書かない。
SE036 disagree。 劣化はテストに含まれている。
SE037 落下試験を含めるべきか？→含めない。
IT039 他の規格が同等かより厳しいかを説明するのはメーカー責任・選択である。
19014-3 以外を使用してもよいが，説明は必要。
19014-3 は最低線であり，メーカ判断でもっと厳しい試験をするのは自由。
US042 inorganic dust → dust とする。
JP047 Chemical Resistance と Salt Spray はクラス C に変更。他の二つはクラス A であるべきとされた。
JP050 ランダムは必須。正弦波を追加でやるのは自由。エンジンのような対象に，主要な周波数を調査する目的で実施するのは意味があると思われる。
JP052 OK。規格の文章が「ランダム振動は実機波形を使ってよい」となっている。
JP056 グラフが正しい。ISO 16750 の 1/10 としている。テーブルの 2 列目（G^2/Hz）は削除する。
JP060 元の規格に熱容量を考慮する，とあるのでそのまま引用する。
JP062 変化速度は重要でないので should にする。

Part 4（ドラフト N0141）

4.4 software module design and coding
－use of trusted component
購入品に広げてもよいか？の議論があった。
6.3 software partitioning
－No priority based scheduling
wrong allocation of processor execution time の対策になっているか？
IEC 61508 にもそうなっているようだが？？

以上