

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 5 月東京 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 2016 年 5 月に東京で開催され、協会標準部会 ISO/TC 127 土工機械委員会から前回 3 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 28 年 5 月 10 日 (火) ~ 13 日 (金)
- 2 **開催地:** 東京都港区 機械振興会館 地下会議室
- 3 **出席者:** 17 名

米国 コンビナー, Part 2 プロジェクトリーダー,
Part 3 プロジェクトリーダー, 他 1 名
英国 Part 1 プロジェクトリーダー, 他 1 名
イタリア Part 4 プロジェクトリーダー
オーストラリア Part 5 プロジェクトリーダー
日本 9 名

4 決定事項

Part 1 (リスクアセスメントの方法と MPLr の割り当て)

前回 2016 年 3 月の Ad hoc 会議で考案したリスクグラフに変更し、DIS 投票に進む。

プロジェクトリーダーは 2016 年 6 月までに DIS 案文を ISO 中央事務局に送る。

その後の予定は ISO 中央事務局次第だが、予想として投票開始 2016 年 9 月、投票締切 2016 年 11 月 (3 ヶ月)

リスクアセスメントの実施例 (現在は ISO/TS 15998-2 の Annex A に記載) は Part 5 として分離し、TR (技術報告書) として作成する。Part 5 の分離は 2016 年 6 月期限で委員会内部投票 (CIB) が進行中。投票については賛成でよいと思う。Part 1 と Part 5 については 7 月に Ad hoc 会議招集 (米国ピオリアで開催)。

Part 2 (制御システムの実装と評価)

CD 投票に進む。プロジェクトリーダーは 2016 年 6 月までに CD 案文を ISO 中央事務局に送る。規格作成のマイルストーンは Part 1, Part 3 と同じで 2016

年 6 月が DIS 案文の作成リミットだが、ISO 中央事務局に対して 9 ヶ月の期間延長を申請中。CD 投票には進むが、電気電子以外の制御システムに対する案文ができていないので CD 投票と並行して案文作成を行う。このため、2016 年 7 月 (米国ピオリアで開催) 及び同 8 月 (イタリア国ローマで開催) に Ad hoc 会議を招集する。

Part 3 (耐環境性要求)

CD に対するコメントを受け入れ、DIS 投票に進む。日程は Part 1 と同じ。「5.6 (ランダム振動の試験) の試験条件の案文を DIS コメントとして提出」が日本宿題となった。

日本が提出した意見「温度サイクル試験 (5.8) はコントローラの設置場所を考慮すべき」は受け入れられ、ISO 15998-1 と同じ文言: “For special operating conditions of the machine and installation conditions of the electronic parts, other environmental conditions may be specified by the manufacturer.” が追記されたが、「全ての試験について試験条件は推奨条件とする」は却下された。

Part 4 (ソフトとバス通信に対する要求事項)

2016 年 7 月までに WD コメント提出のこと。同 8 月に Ad hoc 会議招集 (前記の如くイタリア国ローマで開催)。

その他

2016 年 11 月に WG 24 の全体会合を行い (米国マイアミの予定)、Part 2, Part 4, Part 5 の作業を行う。

ISO 19014 を EN/ISO 19014 として作成する提案がされたよう (N 123) だが詳細不明。EN/ISO となること自体は賛成してよいと思う。

5 日本のアクション

Part 1

パラメータのうち C (Controllability) が他の規格にない独自の決め方になっており、これが最終的な MPLr に大きく効いてくる。ドラフトがほぼ確定したので、日本としては DIS 投票が始まる 2016 年 9 月中頃までに最新案文に基づくリスクアセスメントを各社で試行し、その結果を持ち寄り、投票方針を決める。

Part 2

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, 電気電子を用いない制御系について(意見あれば)CD コメントを提出する。

Part 3

ランダム振動の試験条件の案文を DIS コメントとして提出する。

Part 4

(意見あれば) WD コメントを提出する。

6 議事メモ

Part 1

2016 年 3 月の Ad hoc 会議で考案された修正案が採択された。

・ Exposure

E0	E1	E2
<1%	>1 to <10%	>10%

サービスマンについて

1 人のサービスマンが複数の機械をメンテナンスする場合, exposure はその台数を乗ずるのか? 要検討とされた。

・ Controllability

C0 から C3 の 4 段階であるが, 下記のような ISO 19014 独自の選択方法が採択された。

ISO 19014-1:2016(DIS)

The classifications C0, C1, C2 and C3 represent —easily controllable, —simply controllable, —mostly controllable and —none (see Table 3).

Table 3 – Scores to calculate controllability

Alternative actions / controls to mitigate failure	Awareness level of failure	Ability to react	Admin controls / site management
Yes (1)	High (3)	Good (3)	Always good, enforced by law (1) or not relevant
	Some (2)	Some ability (2)	
No (0)	Low (1)	Low (1)	relevant but Sometimes good / some enforcement (0.5)
	None (0)	Very low (0)	

The above scores in table X are multiplied to achieve the relevant category for controllability.

For example; Yes = 1, High Awareness = 3, Ability to react, Good = 3, admin controls, not relevant = 1

$1 \times 3 \times 3 \times 1 = 9 = C0$ as shown in table X

Table 4 – Possible avoidance of harm

Category	Score – when admin controls are relevant
C0	9
C1	6
C2	≥ 4.5
C3	< 4.5

・ リスクグラフ

			C0	C1	C2	C3
S0			QM	QM	QM	QM
S1	E0		QM	QM	QM	a
	E1		QM	QM	a	b
	E2		QM	a	b	c
S2	E0		QM	QM	a	b
	E1		QM	a	b	c
	E2		a	b	c	d
S3	E0		QM	a	b	c
	E1		a	b	c	d
	E2		b	c	d	e

Figure 1 Determination of PLr

Key

S = severity

E = exposure to hazardous event

C = controllability

QM = quality management system

a, b, c, d, e = required Machine Performance Level MPLr

ベースとなった ISO 25119（農業機械の機能安全）では C0 に対しては QM となっているが、S や E の数値が大きい（リスクを大きくする）場合に QM は不適当という意見が多く、ISO 19014 では MPLr が a や b になる場合がある。ただし、C の定義が変わっているため、単純な比較はできない。

ISO 26262（自動車の機能安全）や ISO 25119 といった自動車系の規格では S、E、C のいずれかが最低レベルならば QM がつく（ISO 25119 は一か所だけ a がつく）が、ISO 13849 の思想（安全システムなら何らかの要求があるべき）に合わせるべきという意見の影響か、QM が減らされている。

・ Annex C — 警報、インジケータ

現在の案文では、警告やインジケータでは MPL を評価しないこととなっているので良いのだが、今後、高機能な警報装置の出現が予想されるため、そのような警報やインジケータに本規格を適用すべきかどうかの議論があった。

Part 2

- ・ CPU は well-tried とは言えないが、medium-tried 又は almost (?) -tried 等として扱ってはどうか。
- ・ 本文で参照していない Annex L (Joined systems alternative compliance method) は削除。
- ・ Annex D に DC (Diagnostic Coverage) と SFF (Safe

Failure Fraction) の2つの指標が書かれているが、同一であればいずれか削除しては、との意見が出た。計算式としては違うもので、ISO 13849 をベースにするなら SFF は不要と思われるが結論は出ず、CD 案文には残し、不要であればコメント提出することとなった。

Part 3

・ランダム振動 (5.6)

日本が提出した CD コメント「試験条件はコントローラ搭載位置により変えるべき」が受け入れられた。代わりに試験条件を提案するよう要請され、了承した。搭載場所としては、少なくとも cab, chassis, engine, transmission を想定する。

・温度サイクル試験 (5.8)

決定事項に述べた文章追加の他、サイクル数が 50 から 20 に変更された。

・熱衝撃試験 (5.10)

transition time の記述が削除された。

Part 4

・ソフト開発手法の推奨記号について、IEC 61508 の HR/R/O/NR ではなく、+/o/x とする。

要求と要求でないものを明確にするため。

+ : 特定の MPLr に対して選択必要な手法

o : 特定の MPLr に対して規格としては推奨も反対もしない手法

x : 特定の MPLr に対して選択は不適当な手法

- ・ Formal Method (形式手法) は建設機械業界としては導入経験が無く、ツールも市販されていないという認識で一致。WG 24 としては、この手法が存在していることは認識しているが、業界に対して推奨も否定もできないので、Formal Method に対しては中立の立場ということで「o」記号とする。
- ・ モジュールテストにおいて statement coverage や branch coverage 100% は必須としない。
- ・ static resource allocation (Annex A, A29) の定義にスタックが含まれそうな気がするが、除外したほうがよいのではないかと。→次回会議までに案を検討。
**の条件のもとに許す、など。MISLA 等を調べる。
- ・ バス通信については、要求事項が不明確なので MPLr に応じた要求にする等の修正をすべき。記述の仕方に意見があればコメント提出のこと。

以上



ISO/TC 127/SC 2/WG 24 会議風景