

国際標準化活動報告

IEC/SC65A/MT61508-1/-2

IEC/SC65A/MT61508-3

機能安全の紹介

IEC/TC65国内委員会

1. はじめに

機能安全の国際標準化活動を紹介する。機能安全とは、安全機能（電気・電子あるいは機構的な仕組み）を付加することにより、危険事象の発生頻度・被害程度（リスク）を許容可能なレベルまで低減させる考え方のことを言う。例えば、工場の緊急停止装置や鉄道の信号制御装置などの安全機能が該当し、その安全機能はリスク低減の目標に応じた性能が求められる。機能安全規格ではその性能規定を行っている。

産業分野における機能安全規格として、IEC 61508 (Functional safety of electrical/electronic/programmable electronic safety-related systems) の第1版 (Edition 1.0) が1999年から2000年にかけて、第2版 (Edition 2.0) が2010年に発行された。Part 1～Part 7の構成からなる全体で600ページに近い大規模な規格であるが、IECの安全に関連する規格の中で基本安全規格 (basic safety publication) に位置付けられる規格であり、プロセス産業、産業機械、鉄道、自動車、など、他の分野規格や製品規格からも幅広く参照され、産業分野における最も重要な規格の一つである。IEC 61508のパート構成を表1に示す。

IEC 61508は、プロセス産業分野での重大事故が契機となり技術開発と標準化が進んだ背景から、TC65/SC65A (システム一般) が担当しており、SC65Aの直下に設置されている2つのMT (メンテナンスチーム：後述) が現在、第3版 (Edition 3.0) を審議している。メンテナンスとは、国際規格として発行済みの規格を保守・更新するための規格文書を定期的に見直しする作業である。TC65国内委員会は、これらのMTに国際エキスパートを派遣し、積極的に活動している。本稿では、IEC 61508の第3版 (Edition 3.0) に向けての2つのMTにおける審議内容や国際会議の様子を中心に紹介する。

表1 IEC 61508 のパート構成

パート	表題	
Part1	General requirements	一般要求事項
Part2	Requirements for electrical/electronic/programmable electronic safety related systems	電気・電子・プログラマブル電子安全関連系に対する要求事項
Part3	Software requirements	ソフトウェア要求事項
Part4	Definitions and abbreviations	用語の定義及び略語
Part5	Examples of methods for the determination of safety integrity levels	安全度水準決定方法の事例
Part6	Guidelines on the application of IEC 61508-2 and -3	Part2及びPart3の適用指針
Part7	Overview of techniques and measures	技術及び手法の概説

2. 機能安全関連のTC65国際標準化体制

図1に示すように、システム一般を担当分野とするSC65Aの下にIEC 61508の修正や改訂を担当する2つのMTが設置されている。

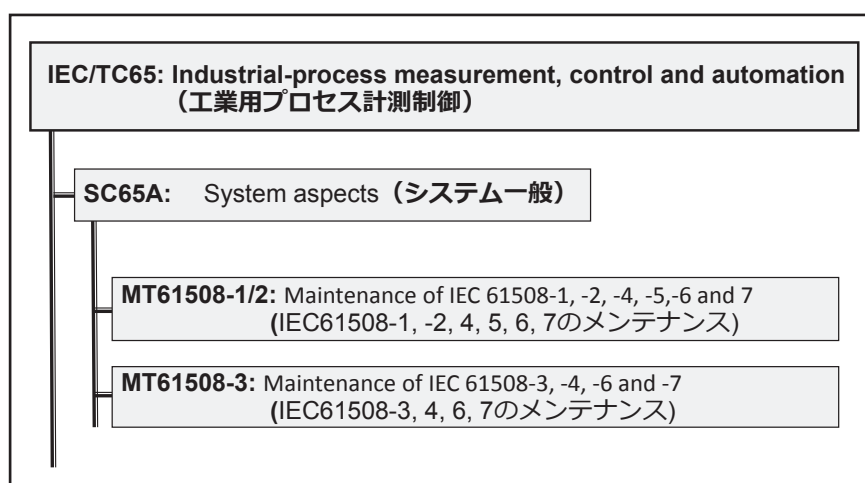


図1 SC65AのMT61508関連の体制

MT61508-1/-2はシステムおよびハードウェアに関するPart 1, 2, 4, 5, 6, 7を扱い、MT61508-3はソフトウェアに関するPart 3, 4, 6, 7を扱っている。双方に関連するPart 4, 6, 7は双方のMTで扱っていることになる。全体や機能安全管理を扱うPart1、システムおよびハードウェアを扱うPart2、ソフトウェアを扱うPart3のようにIEC 61508が扱う分野は多岐にわたっており、それぞれの国際エキスパートの得意分野も分かれるため、上記の2つのMTに分かれてメンテナンス作業を行っているが、両方のMTに登録している国際エキスパートも多い。TC65国内委員会からも、MT61508-1/-2に8名、MT61508-3には11名が国際エキスパート登録をしており、うち8名は両方のMTに登録して活躍している。

以降で、MT61508-1/-2とMT61508-3とに分けて、活動の状況を説明する。

3. SC65A/MT61508-1/-2

表2に、現在までのMT61508-1/-2の国際会議の一覧を示す。

表2 現在までに開催されたMT61508-1/-2の国際会議

回	開催場所	時期	主な内容
1	ロンドン、イギリス	2017/6/13-14	キックオフ、 65A/838/INFのコメント審議 TG (タスクグループ) の設置
2	ジュネーブ、スイス	2017/11/9-10	65A/838/INFのコメントの TG への割り当て
3	リムリック、 アイルランド	2018/3/1	各TGの進捗確認
4	サンクトアウグスティン、 ドイツ	2018/7/4-5	各トピックの審議
5	グルノーブル、フランス	2018/11/14-15	各トピックの審議

IEC 61508第3版 (Edition 3.0) を審議するMT61508-1/-2の活動は、2016年1月の65A/818/DCによる呼びかけから始まった。第3版に向けて改定プロセスの要否、第2版からの修正箇所、新たに盛り込むべきトピックなど、幅広くコメントが募集された。TC65国内委員会からは21件のコメントを提出した。結果、各国より300件程度のコメントが寄せられ、それらをまとめた65A/838/INFが2017年4月に回付された。

キックオフとなる第1回国際会議は、この65A/838/INFで寄せられた各コメントに対する審議を行う目的で、イギリスのロンドンで開催された。MT61508-1/-2は、この300件程度のコメントすべてを、“基本的に合意/レビュー必要/却下”などに分類し、トピック毎にTG (タスクグループ) を設置し、以降、TGを中心に第3版に向けての提案を考えていくこととなった。また、MT61508-3との協調が必要なトピックについて

ては、JTG（ジョイントタスクグループ）を設置した。表3に主なTGを、表4に主なJTGを示す。

表3 MT61508-1/-2 の主な TG

番号	タスクグループ名称	主な論点
1	Complex Semiconductors	マイクロプロセッサ、ASICなどの半導体 ICの分類やガイドラインの検討
2	Common Cause Failures	共通原因故障 共通原因故障の分類
3	SIL Determination PFD/PFH Criteria	安全度水準の決定手法 要求SILの決定方法
4	Reliability Modelling guidance	信頼性モデルガイドライン Part6の全面的な見直し
5	EMC and functional safety	電磁両立性（EMC） EMCの要求事項

表4 MT61508-3 との主な JTG

番号	タスクグループ名称	主な論点
1	Proven-in-use concept	使用実績による証明 ソフトウェアへの要求事項とハードウェアへの展開
2	Hardware/Software Interface	ハードウェア/ソフトウェア インタフェース Part2/Part3間でのインタフェースの規定
3	Cyber security and safety	サイバーセキュリティと安全 サイバーセキュリティに対する要求事項
4	Tool Qualification	開発ツール ソフトウェア、およびハードウェアの開発ツールの扱い

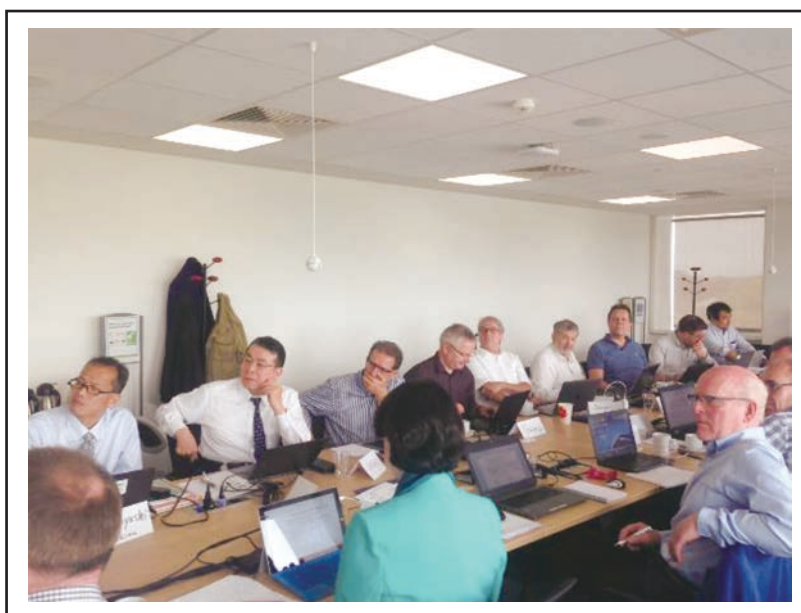


写真1 第1回 MT61508-1/-2 会議の様子（ロンドン、英国）

なお、正式な改定プロセスはまだ開始しないことが確認され、当面、非公式な作業として検討を進めていくこととなった。

第2回の国際会議はスイスのジュネーブで開催され、65A/838/INFの各コメントを各TGへ割り当てた。各タスクグループは、割り当てられたコメントに対する改定内容の提案を行っていくことが確認された。

以降、TG毎にトピックを審議、ならびに改定内容の検討が続いているが、回を重ねる毎に参加する国際エ

キスパートメンバーも少しずつ増える傾向にあり、各エキスパートの観点・論点の違いから、トピックによっては議論が発散する場面が多くなっている。議論の活発なトピックとしては、サイバーセキュリティ、開発ツール、半導体、信頼性モデルガイドラインなどがあり、例えばサイバーセキュリティでは、セキュリティに関する項目を要求事項として盛り込むべきか否かで盛んな議論が行われており、各国からの注目度の高さがうかがえる。各TGでは改定のスコープから検討することが改めて確認された。

第5回の国際会議はフランスのグルノーブルで開催され、2020年3月までにCD（委員会原案）完成を目指す目標を確認した。なお、MT61508-3と協調しながら、Part 1～Part 7を同時にリリースする方向でいくことも併せて確認した。

今後は、CD作成に向けて作業を進めていくことになる。次回以降の国際会議は、2019年3月にフランス、2019年6月に米国、2019年9月にイギリスでそれぞれ予定されており、CD作成に向けて議論や作業が加速していく見通しである。

4. SC65A/MT61508-3

表5に、現在までのMT61508-3の国際会議の一覧を示す。

IEC 61508の第3版（Edition 3.0）を審議するMT61508-3の活動は、MT61508-1/-2よりも1年半ほど早く始まっている。ソフトウェアの使用実績による証明（Proven in use）に関する提案65A/694/NPが2014年3月に回付され、投票とコメント募集が実施された。この提案はソフトウェアの使用実績による証明（Proven in use）に対する技術仕様書TS（Technical Specification）（TS 61508-3-1）の発行を目的とする。TC65国内委員会は賛成票と積極的なコメントを提出した。TSのスコープがあいまいであるという問題点に対する解決方法の提案を始め、要求事項を明確にするための技術的なコメントなど、全24件のコメント中、TC65国内委員会からのコメントが最大の13件という結果となった。2014年9月には投票結果が65A/705/RVNとして回付され、提案は賛成多数で可決された。

表5 現在までに開催された MT61508-3 の国際会議

回	開催場所	時期	主な内容
1	フランクフルト、ドイツ	2014/11/19-21	キックオフ 65A/705/RVN のコメント審議
2	トゥールーズ、フランス	2015/3/17-18	各トピックの審議
3	ロンドン、イギリス	2015/6/9-10	各トピックの審議
4	ヴェステロース、スウェーデン	2015/9/17-18	各トピックの審議
5	フランクフルト、ドイツ	2015/11/3-4	65A/752/CC のコメント審議
6	東京、日本	2016/4/5-7	各トピックの審議 MT61508-1/-2との協調項目抽出
7	ヘルシンキ、フィンランド	2016/9/6-8	各トピックの審議
8	ウィーン、オーストリア	2016/11/30-12/2	各トピックの審議
9	ミラノ、イタリア	2017/4/4-6	各トピックの審議 MT61508-1/-2コンペナーと情報共有
10	ミルウォーキー、米国	2017/9/27-29	65A/838/INFのコメントレビュー TG（タスクグループ）への割り当て
11	リムリック、アイルランド	2018/2/27-28	各トピックの審議
12	サンクトアウグスティン、ドイツ	2018/7/2-3	各トピックの審議
13	グルノーブル、フランス	2018/11/12-13	各トピックの審議

キックオフとなる第1回国際会議は、この65A/705/RVN に対するコメント解決を行う目的で、ドイツのフランクフルトで開催された。MTの初回会議では、日本が24件ともっとも多くコメントを提出し、その議論に多くの時間を費やした結果、その多くのコメントが採用された。この会議では、日本がコメントに関する説明や議論をリードしたため、日本のプレゼンスと貢献を示すことができた。なお、IEC 61508の第3版

(Edition 3.0) は、技術の進歩やソフトウェア開発の現状の実態を踏まえたうえで、広い範囲で検討を始めることになった。主なトピックは、アジャイル開発、オブジェクト指向、開発サポートツール、サイバーセキュリティなどである。例えばオブジェクト指向では、メモリの動的な利用とその安全性について議論されている。

第2回の国際会議以降、各トピックを継続的に議論した。

第5回の国際会議（ドイツ、フランクフルト）では、65A/752/CC（先のTS 61508-3-1のCDに対するコメント）における、約70件のコメント解決が完了した。併せてDTS（TSのドラフト）も参加メンバーが作成した。NPに対するコメント解決を行った先の第1回の国際会議に引き続き、日本は大きな貢献を示すことができた。

第6回の国際会議は、2016年4月5日～7日に（一財）日本品質保証機構（JQA）（東京）で開催した。TC65国内委員会メンバーも発表するなど、日本のプレゼンス向上と貢献を示すことができた。各トピックの審議が行われ、さらには、使用実績による証明（Proven in use）、ハードウェア/ソフトウェアインタフェース、サイバーセキュリティと安全、開発ツール、などが、MT61508-1/-2と協調が必要な項目として挙げられ、JTGを設置することになった。



写真2 第6回 MT61508-3 東京会議後の集合写真（コンベナーを囲んで）

第9回の国際会議（イタリア、ミラノ）では、MT61508-1/-2のコンベナーがゲストとして参加して、MT61508-3として考えているMT61508-1/-2と協調が必要な主な項目について情報の共有を行った。このことが、MT61508-1/-2初回会議準備の有益な情報になり、2017年6月のMT61508-1/-2の第1回国際会議開催に貢献した。

以降、MT61508-1/-2の国際会議と同じ週にMT61508-3の国際会議を開催して、足並みを揃えていくことが基本的なスタイルになった。

第13回の国際会議はフランスのグルノーブルで開催され、MT61508-1/-2と同じく、2020年3月までにCD完成を目指す目標が確認された。なお、MT61508-1/-2と協調しながら、Part 1～Part 7を同時にリリースする方向でいくことも併せて確認された。

今後は、CD作成に向けて作業を進めていくことになる。次回以降の国際会議は、2019年3月にフランス、2019年9月にイギリスがそれぞれ予定されており、CD作成に向けて議論や作業が加速していく見通しである。

5. おわりに

TC65国内委員会の活動として、機能安全 IEC 61508第3版 (Edition 3.0) のメンテナンスに関わる国際標準化の最新状況を紹介した。冒頭で述べたとおり、機能安全規格 IEC 61508 は産業分野における最も重要な規格の一つになっている。技術の進歩にともない産業分野が今後ますます複雑化していくことは明らかであり、その中で安全をどのように確保していくのかは、避けてとおることのできない大きな課題である。TC65国内委員会は、本稿で紹介したMT61508-1/-2やMT61508-3の国際標準化活動を通して、日本の意見を国際標準に盛り込み、Connected industries政策に貢献すると共に、最新技術動向や規制制度の動向に関する情報提供や新規格の提案などにより、JEMIMA会員企業のビジネスの拡大に貢献していく所存である。

執筆

IEC/TC65/SC65A/MT61508国内委員会幹事

IEC/TC65/SC65A/MT61508国際エキスパート

関野 宏美 (横河電機株式会社)