JIS

電気・電子・プログラマブル電子安全関連系の機能安全－第3部：ソフトウェア要求事項

JIS C 0508-3：2014

（IEC 61508-3：2010）

（JEMIMA/JSA）

平成 26 年 2 月 20 日　改正

日本工業標準調査会 審議

（日本規格協会 発行）

日本工業標準調査会標準部会 電気技術専門委員会 構成表

	氏名	所属
（委員会長）	大 崎 博 之	東京大学
（委員）	岩 本 佐 利	一般社団法人日本電機工業会
	岩 本 光 正	東京工業大学
	上 原 京 一	株式会社東芝
	大 石 奈津子	一般財団法人日本消費者協会
	長 田 明 彦	一般社団法人日本配線システム工業会
	熊 田 亜紀子	東京大学
	酒 井 祐 之	一般社団法人電気学会
	下 川 英 男	一般社団法人電気設備学会
	鈴 木 篤	一般社団法人日本照明工業会
	住 谷 淳 吉	一般財団法人電気安全環境研究所
	早 田 敦	電気事業連合会
	田 中 智	一般社団法人日本電機工業会
	中 根 育 朗	一般社団法人電池工業会
	原 田 真 昭	一般社団法人日本電線工業会
	飛 田 恵理子	特定非営利活動法人東京都地域婦人団体連盟
	前 田 育 男	IEC/ACOS エキスパート（IDEC 株式会社）
	山 田 秀	筑波大学

主 務 大 臣：経済産業大臣　　制定：平成 12.2.20　　改正：平成 26.2.20
官 報 公 示：平成 26.2.20
原 案 作 成 者：一般社団法人日本電気計測器工業会
（〒103-0014　東京都中央区日本橋蛎殻町 2-15-12　計測会館　TEL 03-3662-8181）
一般財団法人日本規格協会
（〒108-0073　東京都港区三田 3-13-12 三田 MT ビル　TEL 03-4231-8530）
審 議 部 会：日本工業標準調査会　標準部会（部会長　稲葉　敦）
審議専門委員会：電気技術専門委員会（委員会長　大崎　博之）

この規格についての意見又は質問は，上記原案作成者又は経済産業省産業技術環境局 基準認証ユニット情報電気標準化推進室（〒100-8901　東京都千代田区霞が関 1-3-1）にご連絡ください。

なお，日本工業規格は，工業標準化法第 15 条の規定によって，少なくとも 5 年を経過する日までに日本工業標準調査会の審議に付され，速やかに，確認，改正又は廃止されます。

目　次

ページ
序文 1
1　適用範囲 2
2　引用規格 5
3　用語及び定義 6
4　この規格への適合 6
5　文書化 6
6　安全関連ソフトウェアの管理に関する追加要求事項 6
6.1　目的 6
6.2　要求事項 6
7　ソフトウェア安全ライフサイクル要求事項 7
7.1　一般 7
7.2　ソフトウェア安全要求仕様 14
7.3　システム安全のソフトウェアの妥当性確認計画 17
7.4　ソフトウェア設計及び開発 19
7.5　プログラマブル電子装置統合（ハードウェア及びソフトウェア） 31
7.6　ソフトウェアの運用及び部分改修手順 32
7.7　ソフトウェアのシステム安全妥当性確認 32
7.8　ソフトウェア部分改修 34
7.9　ソフトウェア適合確認 35
8　機能安全評価 40
附属書 A（規定）技法及び手段の選択の手引書 41
附属書 B（参考）詳細表 50
附属書 C（参考）ソフトウェア決定論的対応能力の特性 55
附属書 D（規定）適合品目の安全マニュアル－ソフトウェア要素の追加要求事項 89
附属書 E（参考）JIS C 0508-2 と JIS C 0508-3 との関係 92
附属書 F（参考）単一コンピュータ上のソフトウェア要素間の不干渉性を達成するための技法 94
附属書 G（参考）データ駆動システムに付属するライフサイクルのテーラリングの手引書 99
参考文献 103
解　説 104

まえがき

この規格は，工業標準化法第 14 条によって準用する第 12 条第 1 項の規定に基づき，一般社団法人日本電気計測器工業会（JEMIMA）及び一般財団法人日本規格協会（JSA）から，工業標準原案を具して日本工業規格を改正すべきとの申出があり，日本工業標準調査会の審議を経て，経済産業大臣が改正した日本工業規格である。

これによって，**JIS C 0508-3**:2000 は改正され，この規格に置き換えられた。

この規格の一部が，特許権，出願公開後の特許出願又は実用新案権に抵触する可能性があることに注意を喚起する。経済産業大臣及び日本工業標準調査会は，このような特許権，出願公開後の特許出願及び実用新案権に関わる確認について，責任はもたない。

JIS C 0508 の規格群には，次に示す部編成がある。

JIS C 0508-1　第 1 部：一般要求事項

JIS C 0508-2　第 2 部：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

JIS C 0508-3　第 3 部：ソフトウェア要求事項

JIS C 0508-4　第 4 部：用語の定義及び略語

JIS C 0508-5　第 5 部：安全度水準決定方法の事例（改正予定）

JIS C 0508-6　第 6 部：第 2 部及び第 3 部の適用指針（改正予定）

JIS C 0508-7　第 7 部：技術及び手法の概観（改正予定）

日本工業規格　　JIS
C 0508-3：2014
(IEC 61508-3：2010)

電気・電子・プログラマブル電子安全関連系の機能安全－第3部：ソフトウェア要求事項

Functional safety of electrical/electronic/programmable electronic safety-related systems—Part 3: Software requirements

序文

この規格は，2010年に第2版として発行された**IEC 61508-3**を基に，技術的内容及び構成を変更することなく作成した日本工業規格である。

なお，この規格で点線の下線を施してある参考事項は，対応国際規格にはない事項である。

電気及び／又は電子の要素から成るシステムは，その適用分野において，安全機能を果たすために長年使用してきた。一般に，プログラマブル電子系と呼ばれるコンピュータを用いたシステムは，あらゆる適用分野で，安全以外の機能を達成するために用いられているが，次第に安全機能の履行にも使用するようになった。コンピュータシステムの技術を，効果的かつ安全に活用するためには，意思決定を行うための安全の考え方に関する十分な手引書が必須である。

この規格群では，電気・電子・プログラマブル電子（以下，E/E/PE という。）の要素から成るシステムが，安全機能を履行するための全ての安全ライフサイクル業務に対する包括的な扱い方について規定している。この統一した扱い方は，全ての電気的な安全関連系にわたって，合理的かつ整合性がある技術指針を展開するためのものである。主な目的の一つは，**JIS C 0508**（**IEC 61508**）規格群を基本とした適用分野の製品規格などの制定を容易にし，促進することである。

注記1　**JIS C 0508**（**IEC 61508**）規格群を基本とした適用分野の製品規格などの事例を，参考文献（**JIS C 0511**，**JIS B 9961**及び**IEC 61800-5-2**）に示す。

多くの状況下では，安全性は，幾つかのシステムによって達成し，複数の技術（**例**　機械，液圧，空気圧，E/E/PE技術）に依存している。したがって，いかなる安全対策においても，個々のシステム（**例**　センサ，制御機器，アクチュエータ）の要素だけでなく，全システムを構成する全ての安全関連系を考慮しなければならない。このため，この規格群は，一義的にはE/E/PE安全関連系を対象とするが，更にその他の技術を基本とした安全関連系を対象とする安全の枠組みも提供する。

様々な適用分野において，E/E/PE安全関連系を使用した応用を，多岐にわたり，多様な潜在危険及びリスクが存在することによって生じる複雑さに対応するものとして認識している。いかなる適用においても，要求する安全（達成）手段は，その適用に関わる多数の要因に依存する。この規格群は，包括的であるため，今後の適用分野の製品規格などの制定版及び既存規格の改正版において，個々の手段の形成を可能とする。

この規格群は，次の特徴をもつ。

－　安全機能を遂行するためにE/E/PE系を使用する場合の，最初の概念から，設計，実装，運用及び保全