機能安全活用実践マニュアル

別冊 2　ボイラー自動制御装置の機能安全指針への適合証明申請の手引き

平成 29 年度厚生労働省委託

機能安全を活用した機械設備の安全対策の推進事業

平成 30 年 3 月

中央労働災害防止協会

目次

1. 登録適合性証明機関への申請

1.1 申請手続き

ボイラー及び圧力容器安全規則及び労働安全衛生法及びこれに基づく命令に係る登録及び指定に関する省令（以下、省令）第一条の二の四十四の六第 1 項に定める適合性証明申請書（様式第四号の三）と証明に必要となる書類と登録適合性証明機関が定める費用を添えて提出する。

申請者は、申請対象品が単一ロットで数量限定か継続して計画生産されるものかを申請時に明らかにしなければならない。

1.2 申請の時期

適合性証明審査には、当該製造者の内部システムの構築と運用、試験結果の確認などが含まれるため、以下に示す時期に登録適合性証明機関に申請することが推奨される。

- 新規開発の製品／システムの場合は、設計仕様がほぼ固まった段階。
- 既存の製品／システムの場合は、現行品の実力を確認し、設計変更の仕様がほぼ固まった段階。

2. 登録適合性証明機関の審査

登録適合証明機関により次のように審査される。

2.1 適合宣言の妥当性確認

適合宣言と支援文書が JIS C 0508（IEC 61508） シリーズに従い適切に準備されたか否かの審査がなされる。

支援文書の構成例を**図 1**、支援文書リスト概要例を**表 1**、支援文書例を**附属書**に示す。

2.2 製造者監査

申請品が、継続して計画生産される場合、登録適合証明機関は対象製造者に対し監査を行う。

2.3 証明

登録適合証明機関は、2.1 及び 2.2 項の結果を得て、それが「機能安全による機械等に係る安全確保に関する技術上の指針（厚生労働省告示第 353 号、平成 28 年 9 月 26 日）」に適合していることを確認し、省令第一条の二の四十四の六第 4 項に定める適合性証明を行ったことを証する書面（適合証明書、様式第四の四）を申請者に発行する。なお、証明書の付属書には下記事項が含まれる。

- 証明書番号と発行日付
- 申請日、申請者、適合性証明を行った証明員名、実施管理者名
- 参照した規格リスト
- （必要であれば）付属書に使用される用語の定義
- 証明された型式の概要（製品名、商品名、型式、商品の用途と開発の目的など）
- 外観
- 安全状態
- 証明された機能安全の範囲
- SIL 値、SIL 値を達成するための条件
- 証明に使用した図面リスト
- システム要求に対する結果
- 更新時、サーベイランス実施の要否

2.4 証明書の更新

(1)有効期限

証明の有効期限は登録証明機関の定めによる。

⑵更新手続き

- 有効期限内に規格改訂がない場合

  申請者は、有効期限の範囲内に遅延なく登録証明機関が定める様式に必要事項を記入し、登録適合証明機関に必要な手数料を添えて更新手続きを行うこと。

  更新の条件：

  製造者監査に準じる内容で、サーベイランスを受けること、及び、有効期限内における設計変更管理が適切に行われていること。

- 有効期限内に規格改訂された場合

  上記と同じ。但し、関連する支援文書、例えば、改訂された規格に対する適合性を示した文書を添付すること。

  更新の条件：

  製造者監査に準じる内容で、サーベイランスを受けること、及び、規格改訂時の手順に従い適切に内部処理されており、支援文書が改定されていることを登録適合証明機関が確認する。

3. 機能安全プロジェクトの工程

機能安全プロジェクトの工程表の事例を図 2 に示す。

図 2 では、新規開発の製品／システムの例を示しているが、既存の製品／システムの場合には、最初に現行品の実力を確認しておく必要がある。

図 1−支援文書の全体構成例

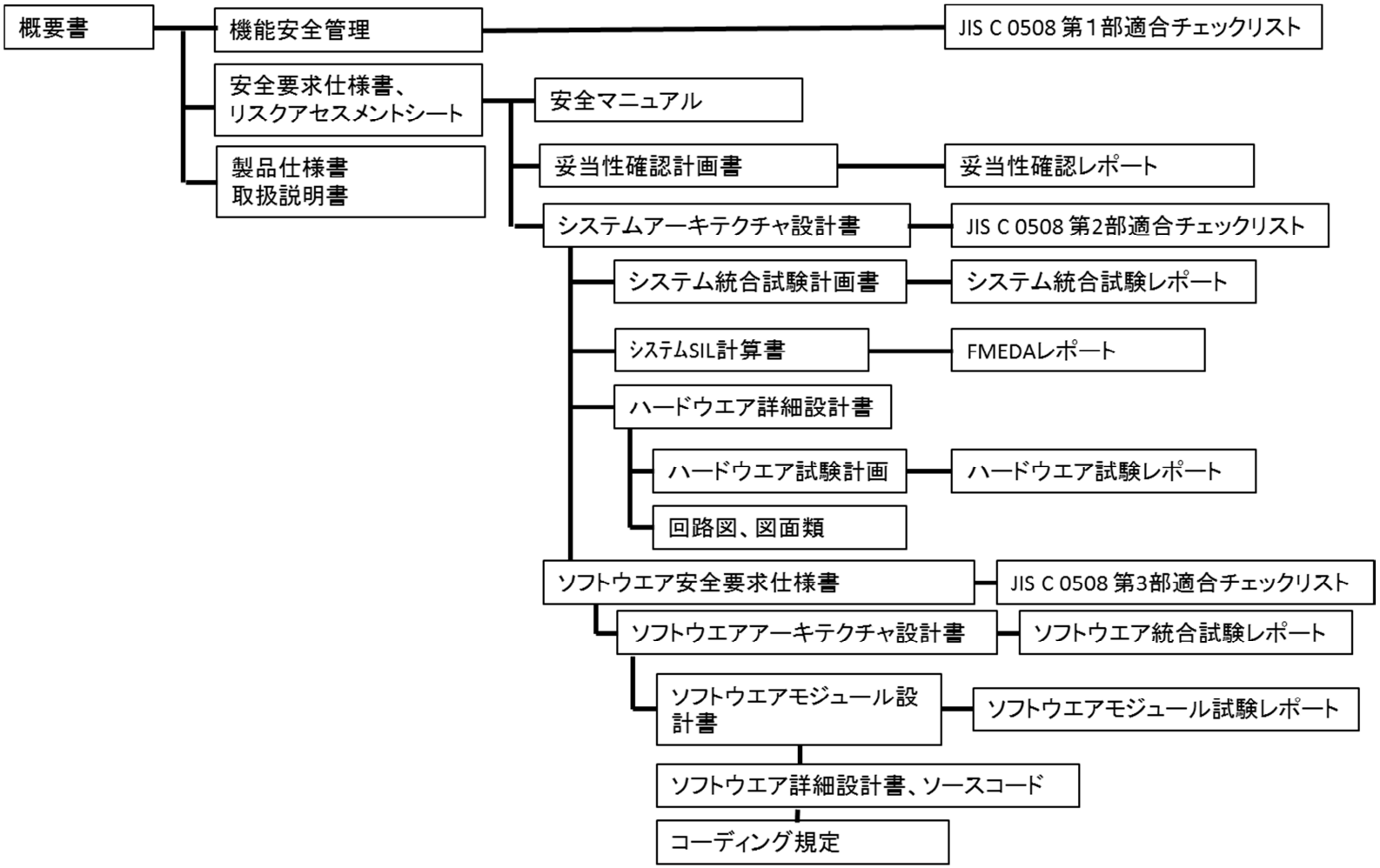


表 1–支援文書リスト概要例

【プロジェクトマネジメントおよびシステム/ハードウエア】

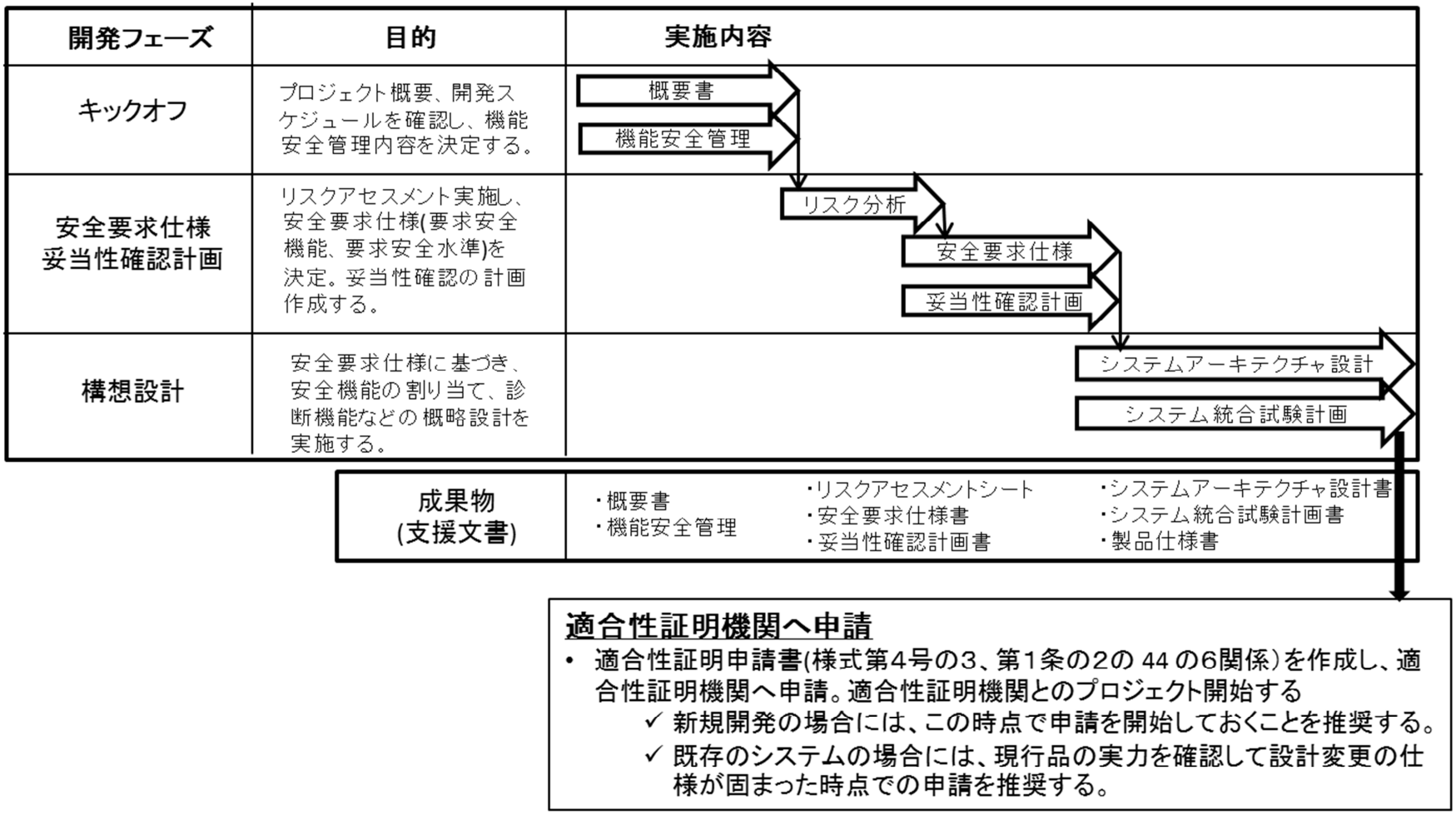
No	タイトル	内容
1	概要書	自動制御装置の概要(申請対象を特定できる型式など、使用できるボイラー仕様)
2	機能安全管理	本プロジェクトの機能安全の方針、組織、品質、管理について規定
3	安全要求仕様書	リスク分析結果､安全要求仕様(安全機能の割り当て、要求安全機能、要求安全度水準)
4	妥当性確認計画書	妥当性確認の計画
5	システムアーキテクチャ仕様書、ハードウエア設計書、	システム構成、安全機能のシステム設計仕様など
6	SIL 計算書、FMEDA 計算書、使用データの出典	SIL 計算書、FMEDA 計算書、使用データの出典
7	図面類	関連図面(回路図、部品リストなど)
8	各テスト計画仕様書とテスト結果レポート	システム統合試験、機能試験、環境試験、EMC 試験、故障挿入試験、など
9	取扱い説明書､安全マニュアル	取扱い、保守、点検マニュアルなど
10	製品仕様書	ボイラー及び自動制御装置の仕様
11	設計レビューなどの記録	開発プロセスの確認
12	妥当性確認結果	ドキュメント、開発プロセス、テストなど全ての要求事項が満たされていることの確認
13	JIS C0508 第 1 部適合チェックリスト	JIS C0508 第 1 部への適合性を証明するチェックリスト
14	JIS C0508 第 2 部適合チェックリスト	JIS C0508 第 2 部への適合性を証明するチェックリスト

【ソフトウエア】

No	タイトル	内容
15	ソフトウエア安全要求仕様書	安全要求仕様のうちソフトウエアに要求される事項
16	ソフトウエアアーキテクチャ設計書	ソフトウエア安全要求仕様に基づく安全機能のアーキテクチャ、ソフトウエア構造、システム結合試験計画
17	ソフトウエアモジュール設計書	単一機能までモジュール化したモジュール設計仕様、モジュール試験計画
18	ソフトウエア詳細設計書 コーディング規定	ソフトウエアの詳細設計仕様、 コーディングルールの規定
19	ソースコード	
20	ソフトウエアモジュール試験レポート	ソフトウエアモジュール試験実施結果
21	ソフトウエア統合試験レポート	ソフトウエア統合試験実施結果
22	JIS C0508 第 3 部適合チェックリスト	JIS C0508 第 3 部への適合性を証明するチェックリスト

図 2-機能安全プロジェクトの工程表例（1/3）

プロジェクト開始から概略設計（3か月）



適合性証明機関へ申請

- 適合性証明申請書(様式第4号の3、第1条の2の 44 の6関係）を作成し、適合性証明機関へ申請。適合性証明機関とのプロジェクト開始する
  - ✓ 新規開発の場合には、この時点で申請を開始しておくことを推奨する。
  - ✓ 既存のシステムの場合には、現行品の実力を確認して設計変更の仕様が固まった時点での申請を推奨する。

図 2-機能安全プロジェクトの工程表例 (2/3)

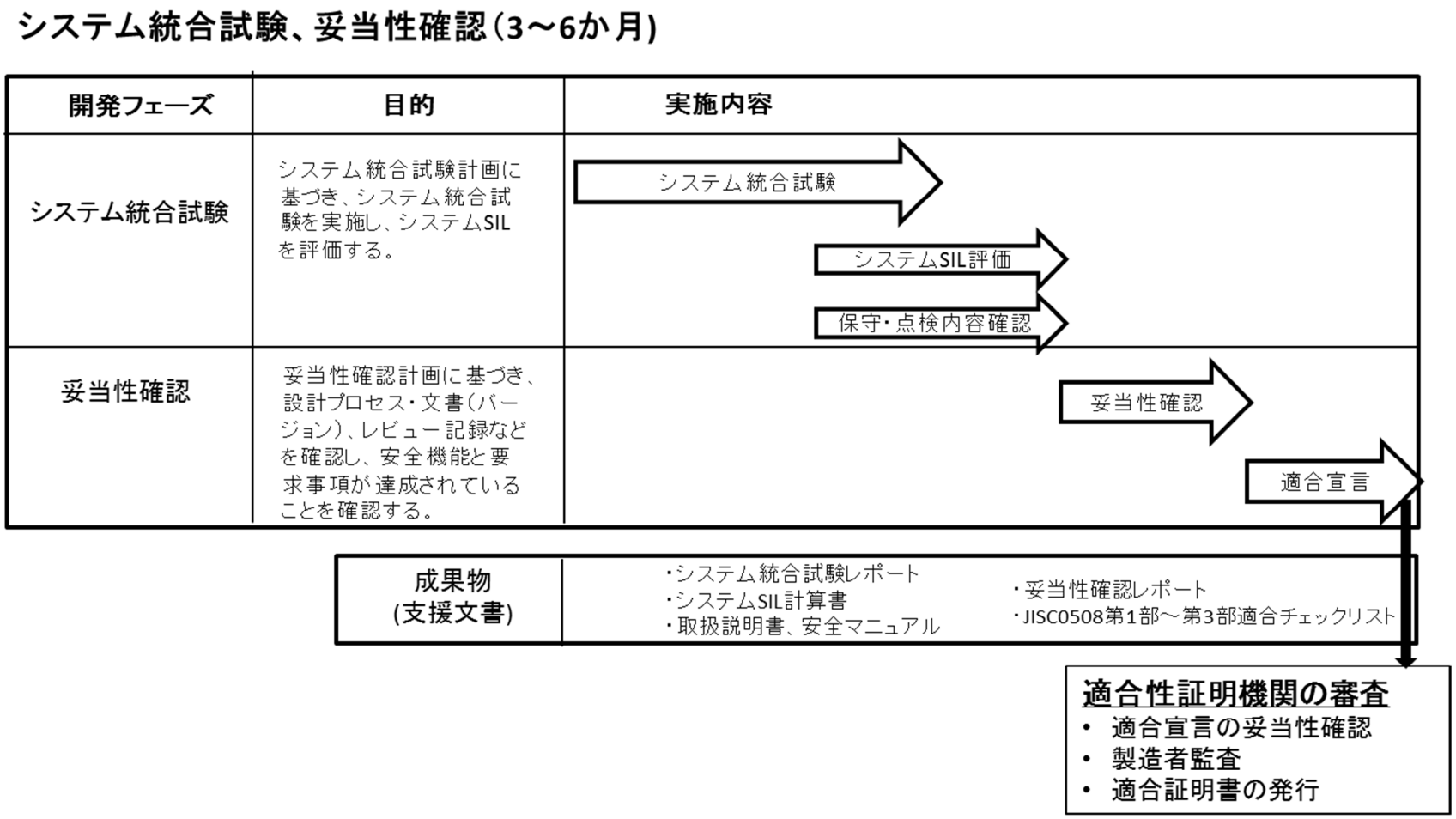
詳細設計(6か月)

開発フェーズ	目的	実施内容(ハードウエア)
詳細設計 (ハードウエア)	システムアーキテクチャ仕様に基づき、ハードウエア設計し、ハードウエア試験実施する。	ハードウエア設計 ハードウエア試験計画 ハードウエア試験 FMEDA
成果物 (支援文書)		・ハードウエア設計書 ・図面、回路図 ・ハードウエア試験計画書 ・ハードウエア試験レポート ・FMEDAレポート

開発フェーズ	目的	実施内容(ソフトウエア)
詳細設計 (ソフトウエア)	システムアーキテクチャ仕様に基づき、ソフトウエア設計し、ソフトウエア試験実施する。	アーキテクチャ設計 モジュール設計 コーディング モジュール試験 統合試験
成果物 (支援文書)		・ソフトウエアアーキテクチャ設計書 ・ソフトウエアモジュール設計書 ・ソフトウエア詳細設計書 ・ソースコード、コーディング規定 ・ソフトウエアモジュール試験レポート ・ソフトウエア統合試験レポート

適合性証明機関によるレビュー
適宜、適合性証明機関によるレビューが実施される。

図 2-機能安全プロジェクトの工程表例（3/3）



附属書 1-【支援文書例：機能安全管理】

機能安全管理

プロジェクト：炉筒煙管ボイラーXX 用自動制御装置

目次

1 本ドキュメントの目的

記載例：

炉筒煙管ボイラーXX 用自動制御装置 XXXX の機能安全管理に関して規定する。

2 プロジェクトの目的、安全方針、品質管理

(対象プロジェクトの目的、安全方針、品質管理について記述する)

記載例：

- 本プロジェクの目的は、炉筒煙管ボイラーXX に使用される機能安全指針に適合した自動制御装置 XXX の開発である。
- 制御対象となるボイラーは、炉筒煙管ボイラーXX シリーズの型式 XXX である。
- 本プロジェクトは、「YYY 開発標準」に規定されたプロセスで実行される。
- 品質マネジメントシステムは、「XXX 品質マニュアル」に従う。
- 本自動制御装置は、SIL3 要求を満たす手法によって開発する。

3 プロジェクトの組織

(プロジェクトの全てのメンバーの役割/責任範囲/経験を記述する)

記載例：

表 1 プロジェクトメンバーの役割と責任範囲

名称	役割と責任範囲	名前	所属組織	経験/スキル
プロジェクトリーダ（PJL）	プロジェクト全体を管理する責任と権限をもつ	AAAAA	CC 部	PJL：5 年 YYY 開発：10 年
機能安全開発リーダ（FSL）	機能安全に関わる開発作業に対して責任と権限をもつ	BBBBB[	DD 部	YYY 開発：10 年 ○○講習受講
・ ・ ・ ・ ・				

4 ドキュメント

4.1 本プロジェクトのドキュメント構成

(本プロジェクトのドキュメントの全体構成を記述する)

記載例：

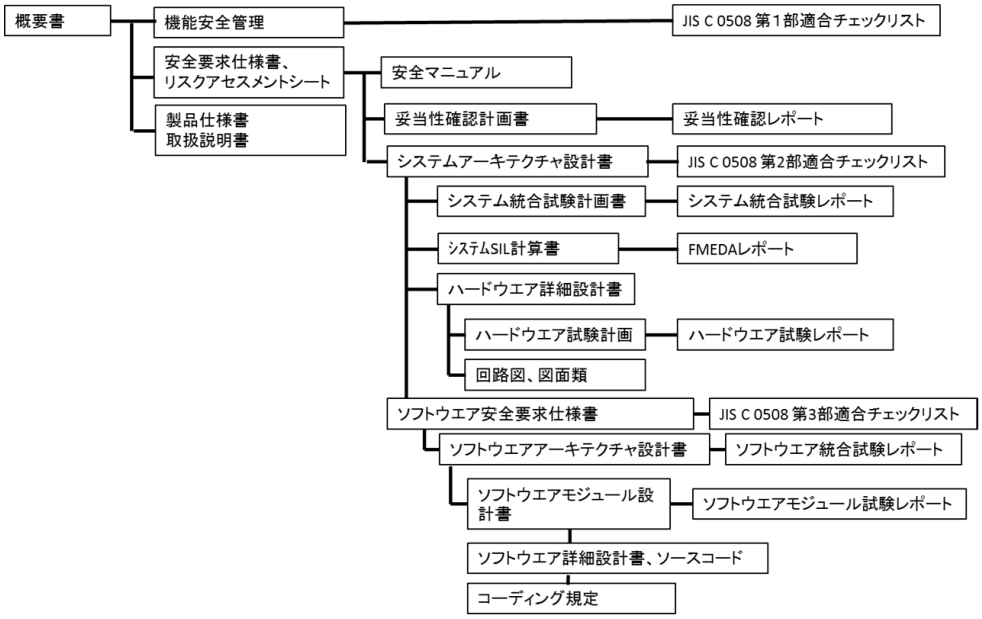


図 1　ドキュメント構成

4.2 社内標準

(本プロジェクトに適用する社内標準/社内規定を記述する)

記載例：

表 2　社内標準/社内規定

No	名称
C-S1	XXX　品質マニュアル
C-S2	YYY　開発規定
・・・	

4.3 適用規格

(本プロジェクトに適用する社外規格、法規制などを規定)

記載例：

表 3　適用する規格/法規

No	名称
平成 28 年厚生労働省告示第 353 号	「機能安全による機械等に係る安全確保に関する技術上の指針」
JISC0508-1,2,3,4,5,6,7	電気・電子・プログラマブル電子安全関連系の機能安全 －第 1 部：一般要求事項 －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 －第 3 部：ソフトウェア要求事項 －第 4 部：用語の定義及び略語 －第 5 部：安全度水準決定方法の事例 －第 6 部：第 2 部及び第 3 部の適用指針 －第 7 部：技術及び手法の概観
・・・・・	

4.4 参照規格および参考文献

(本プロジェクトで技術情報として参照する規格/文献を記述する)

記載例：

表 4　参照規格および参考文献

No	名称
BS EN 13611:2007 + A2:2011	Safety and control devices for gas burners and gas burning applications – General requirements
NPRD-95	Non-electronic Parts Reliability Data (RAC-STD-6200),
JISC1010-1	測定用，制御用及び試験室用電気機器の安全性－第 1 部：一般要求事項
・・・・・	

5 ライフサイクル

5.1 開発プロセス

(本プロジェクトの開発プロセスを規定、ソフトウエアを含む場合にはソフトウエアの開発プロセスも規定する)

記載例：

本プロジェクトは、YYY 開発規定(表 2 C-S1)で規定されている V モデルにしたがった開発プロセスで実施する。

・YYY 開発規定(表 2 C-S1)にしたがったプロセスで実施する

・プロジェクトの組織は、表 1 による。

・SIL3 の要求事項を満たす手法を採用し、実施を確認する。

・YYY 開発規定(表 2 C-S1)で規定されているレビューを実施し、指摘事項の対策完了まで確認する。
・・・・

5.2 ドキュメントリスト

(作成するドキュメントのドキュメント番号，ドキュメントタイトル、作成する開発フェーズなどを記述する)
記載例：

表 5　ドキュメントリスト

No	名称	記述内容概要	作成フェーズ	作成責任者
PJ1-D1	機能安全管理書（本ドキュメント）	プロジェクト概要、関連ドキュメント、機能安全マネジメント、	構想設計	FSL
PJ1-D2	安全要求仕様書	リスクアセスメント、要求安全機能/安全状態、要求安全度水準、	構想設計	FSL
・・・				

5.3 仕様変更／設計変更

(仕様変更/設計変更時のプロセス、インパクトアナリシス(影響解析)の実施などを規定)

5.4 設置/保守

(設置/保守に対する情報提供の方法、市場クレームに対する管理)

6 ドキュメント管理

(タイトル/適用範囲/改訂履歴など必須でドキュメントに記載すべき事項、改番/改訂管理、トレーサビリティ管理、ソフトウエアソースコード/プログラムファイル管理などを規定)

7 プロジェクトで使用するツールなど

(プロジェクト管理、ハードウエア開発/機械設計 CAD、ソフトウエア開発、その他ツール)

8 変更履歴

（本ドキュメントの変更履歴を記載）

改番	日付	変更内容	担当	照査	承認
00	2017/10/01	初版発行	AAA	BBB	CCC
01	2017/12/20	認証機関レビュー結果反映	AAA	BBB	CCC

附属書 2-【支援文書例：安全要求仕様書】

安全要求仕様書

プロジェクト：炉筒煙管ボイラーXX 用自動制御装置

目次

1 目的

記載例：

炉筒煙管ボイラーXX 用自動制御装置 XXXX の安全要求仕様（リスクアセスメントシートを含む）を規定する。

2 リスクアセスメント（潜在危険リスク分析）

2.1 制御対象のボイラー仕様及び使用条件

2.1.1 対象ボイラーの仕様

（本自動制御装置の対象とするボイラーの型式、仕様を列挙、ボイラー系統図など図面も参照する。製品仕様書など別文書で規定していれば、その文書番号と該当箇所を記載する）

記載例：

(1)型式、仕様概要

項目		**仕様**
品名及び型式	ボイラー種類、型式	炉筒煙管式蒸気ボイラー、XX-XXX
仕様・容量	定格蒸発量	18,000（kg/h）
	最高圧力/使用圧力範囲	0.98（MPa）／0.75（MPa）
	蒸気温度	飽和蒸気
	伝熱面積	173.7（m^2）
	燃料/供給圧力	天然ガス／98～294（kPa）
	燃料低位発熱量	40.7（MJ/m^3N）
	バーナ形式	ガス専焼バーナ
	燃焼制御方式	比例制御
	燃焼消費量	1,073（m^3N/h）
	NOｘ値（O_2＝5%換算）	150 ppm 以下
	給水制御方式	比例制御
	使用電源	AC220V
	電気容量	67.5kw

ボイラー系統図は、図面番号 XXXXXX による。

(2)バーナ仕様/燃焼方式

・・・・・

(3)給水制御仕様

・・・・・

(4)燃焼制御仕様

・・・・・

(5)その他制御仕様

・・・・・

2.1.2 ボイラー使用条件

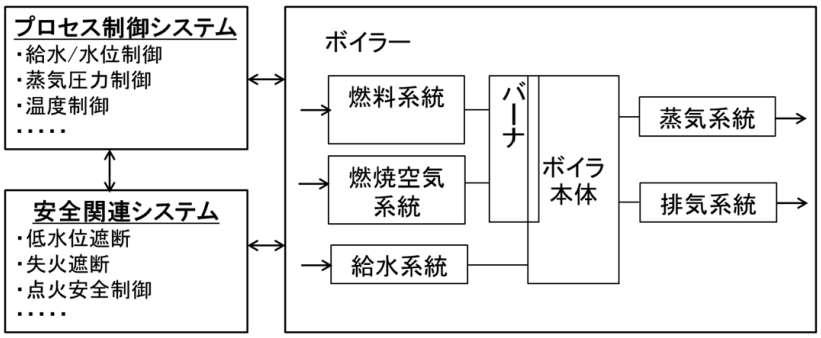
(対象とするボイラーに本自動制御装置を使用した場合の使用条件、保守点検仕様を記述する。取扱い説明書などの別文書で規定していれば、その文書番号と該当箇所を記載する)
記載例：

項目		仕様
使用条件	取扱資格	１級ボイラー技士
	設置場所/設置環境	屋内／非防爆
	運転条件	12 時間／日
保守・点検	日常運転管理	取扱い説明書 NO. XXXXX の X. X 項による
	定期自主検査	1 回／月 (取扱い説明書 NO. XXXXX の X. X 項による)
	性能検査	1 回／年 (取扱い説明書 NO. XXXXX の X. X 項による)
	部品の点検・交換	取扱い説明書 NO. XXXXX の X. X 項による

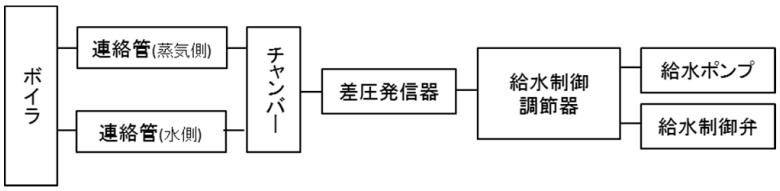
・・・・・

2.2 プロセス制御システムの概要（プロセス制御系と安全関連システム系の区分）

(対象ボイラーのプロセス制御システムを制御系統図と機能ブロック図などで記述する)
記載例：



2.2.1 給水/水位制御の機能ブロック図



2.2.2 燃焼制御の機能ブロック図

・・・・・

2.2.3 蒸気圧力制御の機能ブロック図

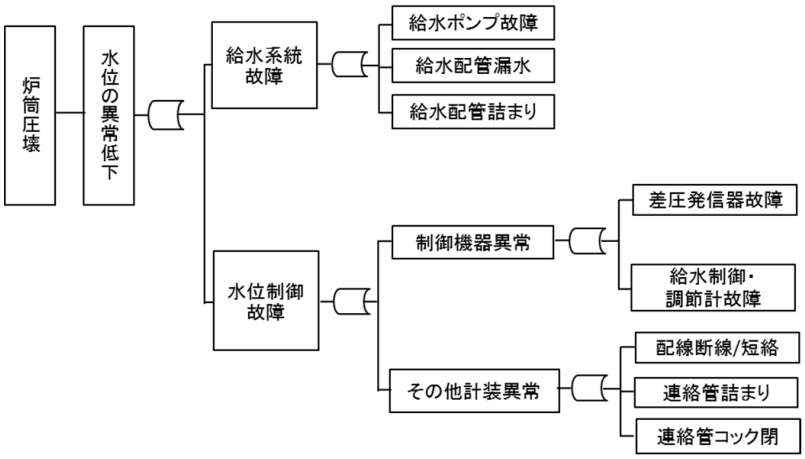
・・・・・

2.3 FTAによる解析

（FTA実施結果を記述する）

記載例：

2.3.1 給水制御系FTA（水位の異常低下）



2.3.2 燃焼制御系統FTA

・・・・・・・

3 要求安全機能、要求安全度水準、使用者への情報

（リスクアセスメントシートの内容により記述する。他書類にて要求安全機能との関連性を記述する際に必要となる場合があるので、それぞれの安全機能毎に番号をつけておく。）

記載例：

表Aリスクアセスメントシートに記載した結果より、以下の通りとする。

3.1 低水位遮断機能（RSF0001）

①安全機能

水位が安全低水位面以下になった場合に燃料遮断する。

②要求安全度水準

SIL2

③検出方法

低水位検出器による（詳細仕様は XXXX による）

④作動要求に関連する事項(対象ボイラーに要求される構造/機械式安全装置

「ボイラーの低水位による事故の防止に関する技術上の指針」の構造要求に適合していること。

⑤使用者への情報提供（使用者追加対策）

・給水圧力、水面計、水位制御機能の日常点検取扱い説明書 XXXX の X.X 項による）

・給水系統の配管,機器からの漏れの日常点検（取扱い説明書 XXXX の X.X 項による）

・連絡管コックの開閉状態の確認（取扱い説明書 XXXX の X.X 項による）

3.2 失火遮断機能（RSF0002）

・・・・・・

3.3 遮断弁閉確認（RSF0003）

・・・・・・

3.4 エア圧力低下（RSF0004）

・・・・・・

・・・・・・

4. 変更履歴

（本ドキュメントの変更履歴を記載）

改番	日付	変更内容	担当	照査	承認
00	2017/10/01	初版発行	AAA	BBB	CCC
01	2017/12/20	認証機関レビュー結果反映	AAA	BBB	CCC

記載例：

表 A　リスクアセスメントシート

要求安全機能の特定							安全度水準決定					取扱説明書記載事項、点検内容など	
No	キーワード	危険側故障	危険事象	検出方法	要求安全機能	作動要求に関する事項 (構造/機械式安全装置)	C	F	P	W	SIL	製造者追加対策	使用者追加対策
1	水位異常低下	給水ポンプ故障	過熱/空炊きによる火災又は圧壊	低水位検出器	水位が安全低水面以下になった場合に燃料を遮断する(低水位遮断)	「ボイラーの低水位による事故の防止に関する技術上の指針」の構造要求に適合	C_D	F_A	P_B	W_1	2	給水圧力計の設置	給水圧力、水面計、水位制御機能の日常点検
2	水位異常低下	給水配管の漏水/詰まり	過熱/空炊きによる火災又は圧壊	No1 と同じ	No1 と同じ	No1 と同じ	C_D	F_A	P_B	W_1	2	No1 と同じ	No1 と同じ
3	水位異常低下	給水ポンプ用電磁開閉器の故障	過熱/空炊きによる火災又は圧壊	No1 と同じ	No1 と同じ	No1 と同じ	C_D	F_A	P_B	W_1	2	No1 と同じ	No1 と同じ
4	水位異常低下	制御用水位検出器/電極棒の故障	過熱/空炊きによる火災又は圧壊	No1 と同じ	No1 と同じ	No1 と同じ	C_D	F_A	P_B	W_1	2	No1 と同じ	No1 と同じ
5	水位異常低下	水位制御系配線の断線/短絡	過熱/空炊きによる火災又は圧壊	No1 と同じ	No1 と同じ	No1 と同じ	C_D	F_A	P_B	W_1	2	No1 と同じ	No1 と同じ
6	水位異常低下	水側連絡管の詰まり/コック閉	過熱/空炊きによる火災又は圧壊	No1 と同じ	No1 と同じ	No1 と同じ 水側連絡管は他の水位検出器の連絡管と分離	C_D	F_A	P_B	W_1	2	No1 と同じ 連絡管は内部掃除が容易な構造	No1 と同じ コックの開閉状態の確認

中央労働災害防止協会　技術支援部　2018.3