機能安全活用実践マニュアル

ボイラー編

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

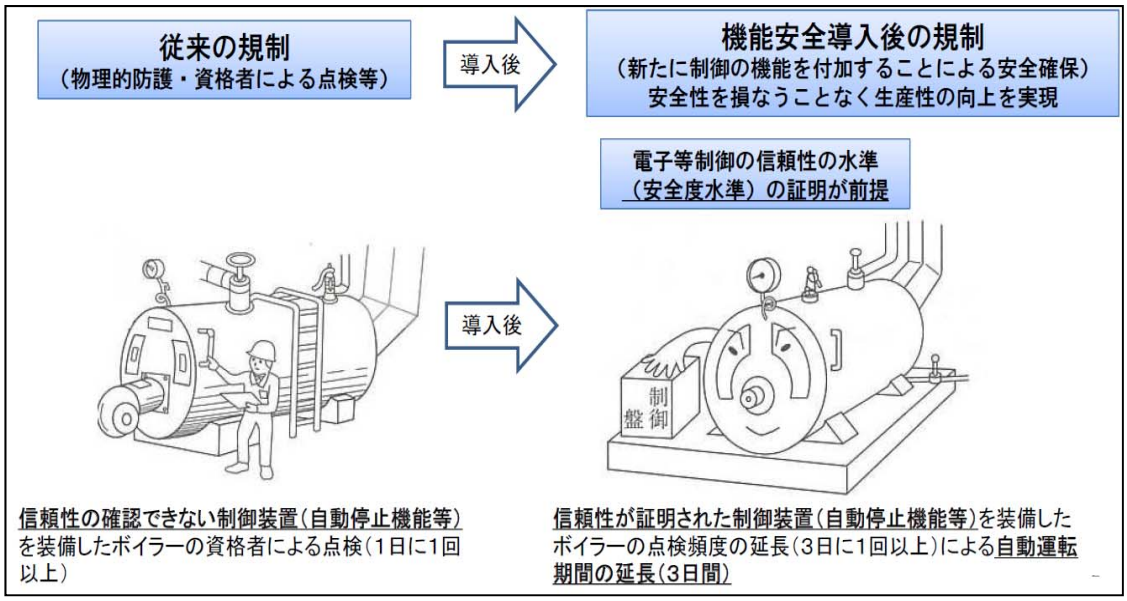
中央労働災害防止協会

目次

はじめに

1. 本マニュアルの目的

平成 28 年 9 月に、「ボイラー及び圧力容器安全規則（以下、「ボイラー則」という。）」、「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、「登録省令」という。）」、「ボイラー及び圧力容器安全規則第 24 条第２項第４号の規定に基づき厚生労働大臣が定める自動制御装置（平成 16 年厚生労働省告示第 131 号。（以下、「自動制御装置告示」という。）」、「ボイラーの遠隔制御基準等について（基発第 0331001 号）」の一部が改正され、同時に、「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（平成 28 年厚生労働省告示第 353 号。以下、「**機能安全指針**」という。）」が新たに公布された。



これらの改正・指針は、従来のボイラーの機械式安全装置などに、新たに電気・電子・プログラマブル電子制御の機能を付加することによって機械等の安全を確保する方策（以下「機能安全」という。）を労働安全衛生関係法令に位置づけ、安全規制の高度化を図るものである。ボイラーは、労働安全衛生関連法令においてボイラー則、構造規格などの様々な安全規制が実行されている。今回の改正では、ボイラー異常時に安全に自動停止する機能を、機能安全指針に適合し認定を受けた自動制御装置で構成することによって、点検頻度、ボイラー作業主任者の選任基準や勤務場所などに対する特例が設けられた。

本マニュアルは、機能安全指針に適合するボイラーの自動制御装置を設計するために、機能安全を導入するための設計段階でのリスクアセスメント及び設計手法などについて、ボイラーにおける具体例を交えてまとめたものである。

なお、本マニュアルは、「機能安全の活用促進に関する検討委員会」の「ボイラーワーキンググループ」において作成され、同委員会で作成された「テキスト編」で事前に学習されていることが前提となっている。

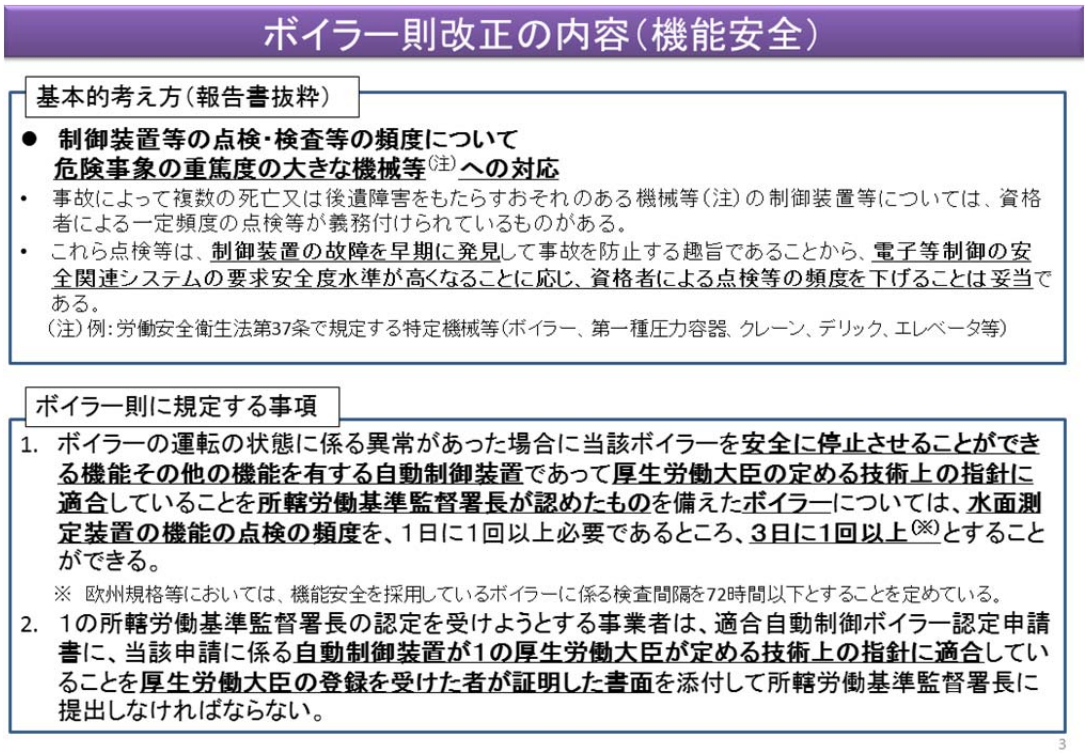
2. 省令などの改正について

（１）水面測定装置の点検頻度の特例に関するボイラー則の改正

ボイラー則第 25 条の改正により、①ボイラーに異常があった場合に、安全に停止させる機能を有する自動制御装置であって、②厚生労働大臣の定める技術上の指針（機能安全指針）に適合していることを③所轄労働基準監督署長が認めたものを備えているボイラーについて、通常１日に１回の水面測定装置の点検の頻度を３日に１回以上とできることを規定した。

機能安全指針に自動制御装置が適合していることについては、厚生労働大臣の登録を受けた第三者の専門機関に、技術上の指針に適合していることを証明してもらい、その証明書を添付して認定の申請をする規定となっている。

さらに、ボイラーの遠隔監視に関する通達（平成 15 年３月 31 日付け基発第 0331001 号）を改正し、労働基準監督署長の認定を受けた自動制御装置を備えたボイラーについては、情報端末を常時携帯することや、３日に１回、ボイラー設置場所で点検を行うなどの一定の条件を満たせば、ボイラー設置場所から１時間程度離れた場所でボイラー技士が勤務することが認められた。



（２）遠隔監視基準の改正

ボイラーの遠隔制御監視基準等の通達も改正され、従来の方法(別添1、別添２)に加えて、別添３が追加された。認定適合自動制御装置を備えたボイラーでは、情報端末を常時携帯することや、３日に１回ボイラー設置場所で点検を行うなどの一定の条件を満たせば、ボイラー取扱作業主任者は、少なくとも１時間程度でボイラー設置場所に到達できる場所で勤務することが認められこととなった。

<table>
<tr><th colspan="2">ボイラーの遠隔制御監視基準等について（基発 0331001 号）</th></tr>
<tr><td rowspan="2">従来の基準</td><td>別添１：遠隔監視室で監視するボイラー
・ボイラー運転中は常時遠隔監視室にて監視
・ボイラー設置場所で１日に１回以上点検</td></tr>
<tr><td>別添 2：有線、構内 PHS 等を用いた監視装置で監視するボイラー
・ボイラー運転中は常時監視装置にて監視
・ボイラー設置場所で 4 時間に１回以上点検</td></tr>
<tr><td>機能安全導入により追加された基準（平成 28 年９月 基発 0930 第 35 号）</td><td>別添 3：認定適合自動制御装置を備えたボイラー
・１時間程度でボイラー設置場所に到達できる場所で勤務
・起動後１時間以内、その後は 72 時間以内ごとに点検
認定適合自動制御装置とは、ボイラーの運転の状態に係る異常があった場合に当該ボイラーを安全に停止させることができる機能その他の機能を有する自動制御装置であって、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（平成 28 年厚生労働省告示第 353 号）に適合していると所轄労働基準監督署長が認定したもの</td></tr>
</table>

（３）ボイラー取扱作業主任者の選任基準の改正

ボイラー則第 24 条(ボイラー取扱作業主任者の選任)の第２項第 4 号に規定に基づき伝熱面積に参入しないことができるボイラーの自動制御装置に関する告示も改正され、認定適合自動制御装置を備えたボイラー(但し最大の伝熱面積を有するボイラーを除く)を伝熱面積の合計に算入しないことが可能となった。(関係告示：厚生労働省告示第 354 号、平成 28 年 9 月)

ボイラー則第 24 条（ボイラー取扱作業主任者の選任）第２項第４号 概要：関係告示（平成十六年厚生労働省告示第百三十一号）で定めた自動制御制御と装置を備えたボイラーは、ボイラーの伝熱面積の合計に算入しないことができる。	
従来の基準	関係告示：厚生労働省告示第百三十一号（平成十六年） ボイラー及び圧力容器安全規則第二十四条第二項第四号の厚生労働大臣が定める自動制御装置は、次の各号のいずれにも該当する自動制御装置とする。一～三　（略）
機能安全導入により追加された基準	関係告示：厚生労働省告示第 354 号（平成二十八年九月） 第二十五条第二項の規定により厚生労働大臣が定める技術上の指針に適合していると労働基準監督署長が認定した自動制御装置 （認定適合自動制御装置）

（４）登録適合性証明機関の新設

「労働安全衛生法及びこれに基づく命令にかかる登録及び指定に関する省令」が改正され、自動制御装置が機能安全指針に適合していることを証明する第三者機関として、「登録適合性証明機関」が新設された。適合性証明機関は、①制御機能が適切に設計されていること、②設計通りに製造されていることをユーザーに対して証明する。

登録省令には、適合性証明機関の登録基準等として、証明者の資格要件を定めるほか、実施義務として、公正な証明などを義務付けた。さらに、機関に対する監督として、適合命令、改善命令の権限を定めるほか、取り消しの規定が設けられ、登録機関による証明の品質確保が図られる。なお、登録証明機関は、ボイラー以外の機械等の電子等制御の機能が機能安全指針に適合していることを証明することも可能である。

労働基準監督署長の認定を受けようとする事業者は、適合自動制御ボイラー認定申請書（ボイラー則様式第 17 号）、「登録適合性証明機関」が証明した適合証明書及び付属書面を添付して所轄労働基準監督署長に申請する。

3. 本マニュアルで使用する用語

機能安全指針に記載されている以下の用語を使用する。なお、ここに記載した用語定義と、ISO/IEC Guide51(JIS Z8051)およびIEC61508-4(JIS C0508-4)の用語定義とは若干の相違があるが、本マニュアルでは、下記の定義を使用する。また、特に記載のない用語に関しては、テキスト及びISO/IEC Guide51(JIS Z8051)、IEC61508-4（JIS C0508-4）に準じることとする。

(1)リスク

機械等による労働者の就業に係る負傷又は疾病の重篤度及び発生の可能性の度合い

(2)機能安全

新たに機械等に電気・電子プログラマブル電子制御の機能を付加することにより、リスクを低減するための措置

(3)製造者

機械等を製造する者

(4)危険事象

機械等による労働者の就業に係る危険性又は有害性の結果として労働者に就業上の負傷又は疾病を生じさせる事象

(5)要求安全機能

機械等による労働者の就業に係る危険性又は有害性を特定した上で、それによるリスクを低減するために要求される電気・電子プログラマブル電子制御の機能。

(6)安全関連システム

要求安全機能を実行する電気・電子プログラマブル電子制御のシステム

(7)要求安全度水準

安全関連システムに要求される信頼性の水準。

要求安全機能の作動が要求された時に、安全関連システムが当該要求安全機能を作動させる確率であり、その水準を表す指標として、IEC61508の安全度水準又はISO13849のパフォーマンスレベルが用いられる。

(8)作動要求頻度

要求安全機能の作動が求められる頻度。

参考URL

厚生労働省：機能安全による機械等の安全確保について

URL: http://www.mhlw.go.jp/stf/seisakunitsuite/bunya/0000140176.html

第１章ボイラーのリスクアセスメント(機械類の制限の決定）

1. ボイラー仕様とリスクアセスメント範囲

(1) リスクアセスメント範囲の指定

ア．対象設備の範囲

リスクアセスメントの開始にあたって、対象ボイラーの仕様を明確にし、リスクアセスメント実施するボイラー設備の範囲を指定することが必要となる。

ボイラーの使用者が実施するボイラー取扱い作業に関するリスクアセスメントでは、周辺設備や補助設備を含んだ形で実施されるが、本マニュアルで扱うボイラーへの機能安全の導入では、ボイラーに異常があった場合にボイラーを安全に停止させる機能を機能安全により確保する、という目的に合致した範囲を指定することが必要である。したがって、本マニュアルで扱うボイラーへの機能安全の導入にあたってのリスクアセスメント範囲としては、ボイラー本体、燃焼装置、自動制御装置、附属装置及び附属品の範囲に限定して実施する。（ボイラー則第 32 条に相当する範囲、表 1-1）

表 1-1　ボイラー則 32 条 定期自主点検項目

ボイラー本体	
燃焼装置	油加熱器及び燃料送給装置
	バーナ
	ストレーナ
	バーナタイル及び炉壁
	ストーカ及び火格子
	煙道
自動制御装置	起動及び停止の装置、火炎検出装置、燃料遮断装置、水位調節装置、圧力調節装置
	電気配線
附属装置	給水装置
	蒸気管及びこれに付属する弁
	空気予熱器
	水処理装置

イ．範囲指定例

図 1-1 に炉筒煙管ボイラーのフロー図の例、図 1-2 に、その自動制御装置系統図の例を示した。

この事例では、給水系統は、原水→原水ポンプ→軟化装置→軟水タンク→給水ポンプ→節炭器→ボイラー本体へとなっている。このうち、原水から軟水タンクまではボイラーとは別系統で制御されており、ボイラーのリスクアセスメントの範囲としては、給水ポンプ以降を対象とする。

燃焼装置は、ガス燃焼のバーナであり、バーナの燃料系統はガス元コック直下のストレーナ―より下流側、通風系統は押込送風機より下流側を対象とする。その他、排

ガス系統は排気ダンバーから節炭器まで、蒸気系統とブロー系統はボイラー直下までとしている。なお、このボイラーには附属装置として薬注装置が設置されているが、薬注装置の異常は軽故障(ボイラーを停止しない故障)と定義されているため、薬注装置は対象外としている。

図 1-1 のフロー図にて対象範囲を明示し、この対象範囲の制御系統を明確にするために、図 1-2 の自動制御機器系統図で対象の制御機器を明示している。このように、リスクアセスメント範囲を明確にするためには、機能安全を導入する自動制御装置系統とボイラー全体の系統で区別できるようにしておくことが重要である。

(2)ボイラーの仕様及び使用条件

ア．型式、仕様

ボイラー種類、型式、一般仕様・容量、制御方式を仕様として定義する。(表 1-2)

表 1-2　ボイラーの仕様(例)

項目	内容	例
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

なお、表 1-2 ではひとつの型式に対する一般仕様のみ記述しているが、異なる仕様のボイラー型式が追加される、あるいは特殊仕様の対応が追加になる可能性があるなら、あらかじめそれらの仕様も記述しておくと、型式追加時の作業が容易になる。その場合には、(1)のフロー図、制御系統図と合わせて、記述を整合化しておくことが必要である。

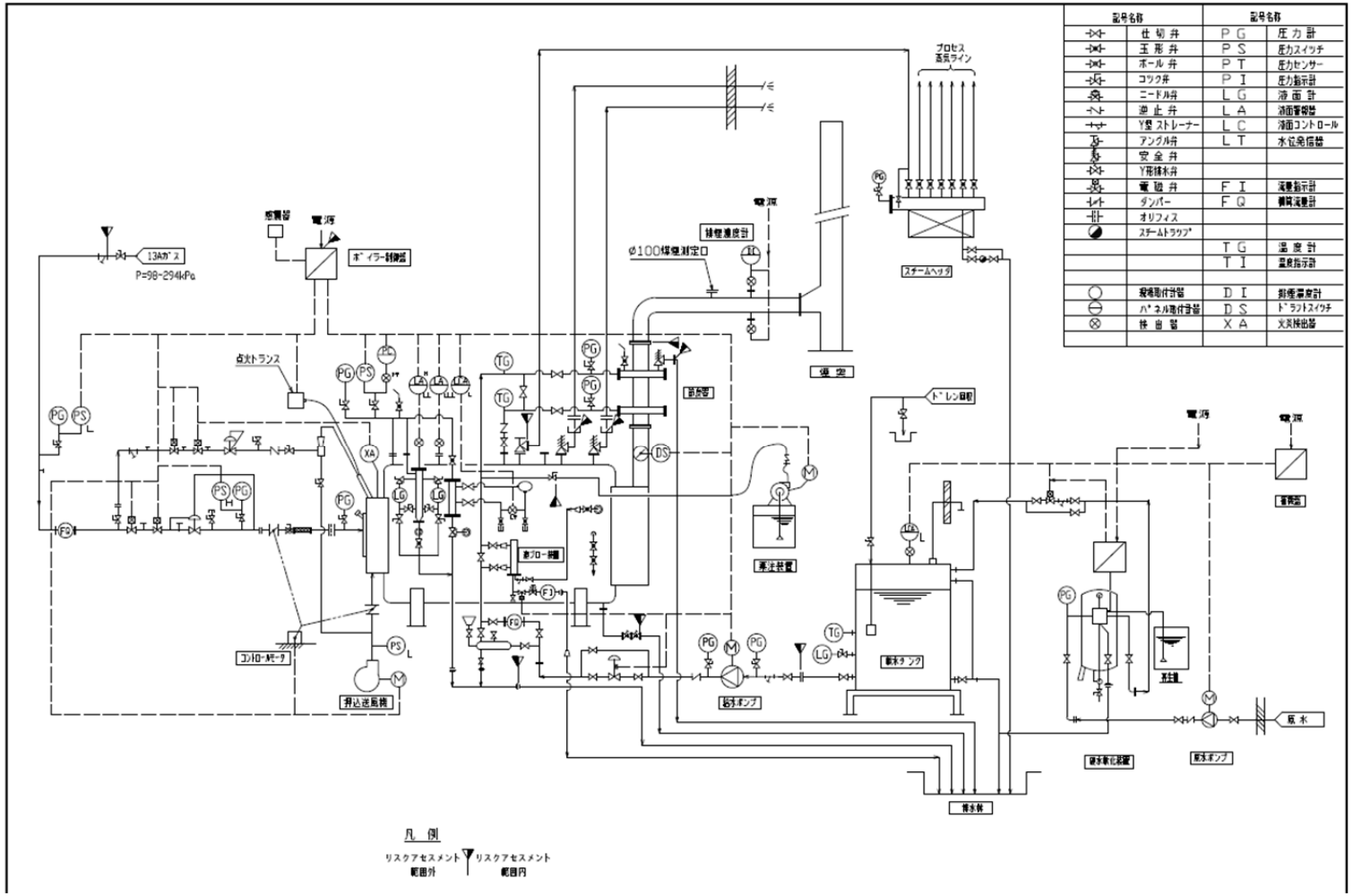


図 1-1 炉筒煙管ボイラーの系統図例

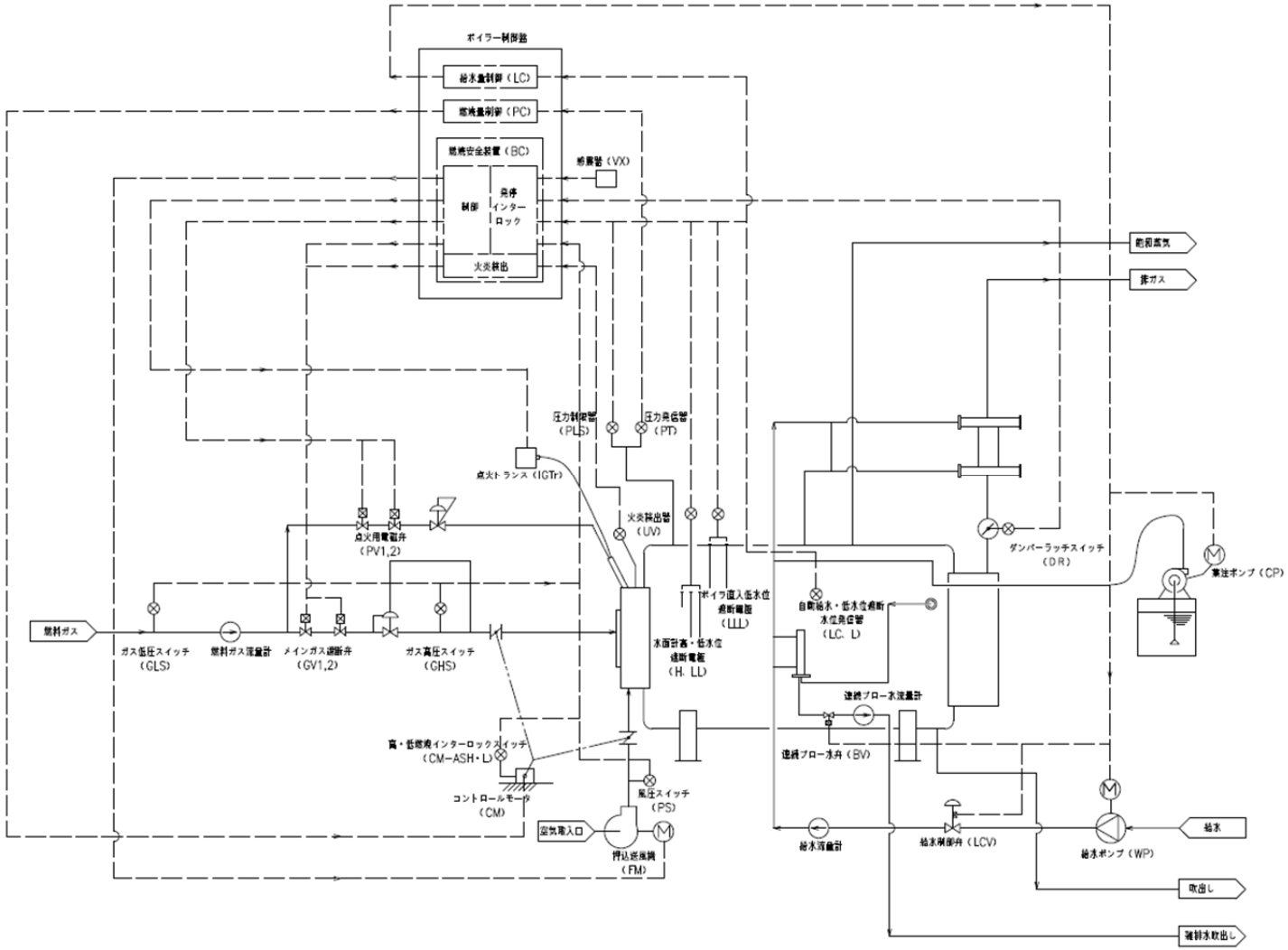


図　1-2　自動制御装置系統図

イ．使用条件

使用条件として、対象ボイラーの取扱い資格を指定し、1 日あたりの運転時間。ボイラー設置場所/設置寛容などの制限仕様を記述する。(表 1-3)

特に、ボイラーの設置場所、設置環境については、危害を受ける可能性のある人が複数以上存在するかどうかを判断する材料となり、安全度水準の決定に大きく影響する要因である。ボイラーの場合、特別に指定された設置場所、設置環境でないかぎり、ボイラーの重故障による爆発等の危険事象では、危害を受ける可能性のある人は複数存在することが前提となる。したがって、危害を受ける可能性のある人が一人以下であると判断した場合には、その判断の根拠となる設置場所・設置環境の要件を明示する必要がある。そうでない場合(危害を受ける可能性のある人は複数存在することが前提の場合)には、一般的な要件として、防爆/非防爆、屋内/屋外の種別程度の記述とする。

また、1 日あたりの運転時間は、ボイラー設計上の要件として決められた時間で規定しておく必要がある。例えば、部品の点検・交換周期を決めた際に想定した 1 日あたりのボイラー運転時間などから決定する。

表 1-3　ボイラーの使用条件、保守点検の例

項目	内容	例
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	別紙参照（取扱い説明書による）
	定期自主検査	1 回／月（定期自主検査指針による）
	性能検査	1 回／年
	部品の点検・交換	別紙参照（取扱い説明書による）

ウ．保守・点検

法令等で定められている性能検査、定期自主検査の実施は必須事項である。その他に、運転開始時/運転中/毎日/毎週などの単位で必要となる日常の運転管理内容を、取扱い説明書などのユーザーに提示する資料で規定する内容にて確認をする。また、部品や制御機器の点検・交換についても、表 1-4 のようにリスト化してユーザへ提示することが必要である。

表 1-4 部品点検・交換リスト例

炉筒煙管式ボイラーにおける寿命の目安

建築保全・1992年3月号・No. 76
出典 建築設備維持研究会資料

機器材料	部位・部材	検出項目	診断技術	判断基準	対応策・処置	耐久性・寿命の目安
本体 胴		腐食	厚さ	構造規格による		15年
〃 管板		〃	〃	〃		15年
〃 炉筒		〃	〃	〃		15年
〃 ステー管		〃	〃	〃		8年
〃 煙管		〃	〃	〃		8年
燃焼 バーナ	バーナチップ	洩れ	油量 発煙 空燃比チエック	メーカー基準による	バーナチップ交換	10年(バーナチップ 2年)
			油温上昇 異音発生			
〃 噴燃ポンプ	ギヤ、パッキン	振動、油圧 洩れ	油圧低下 能力低下	〃	取替	3年
〃 送風機	ベアリング	振動	異音振動発生能力低下	〃	ベアリング交換	10年(ベアリング 4年)
〃 風箱		振動				15年
〃 耐火物		脱落 割れ	目視により耐火物点検		打直(取替)	2年
			異常発生			
給水 ポンプ	ベアリング、パッキン	振動洩れ、水圧	能力低下	メーカー基準による		8年 ベアリング 2年 パッキン 2年
〃 インゼクター		作動	作動不良			8年
制御 圧力調節器	ベローズハウジング	洩れ		メーカー基準による	取替	4年又は、10万回
	ポテンショメータ	振動部の汚れ、粗れ	抵抗値			
〃 圧力スイッチコントロール	ベローズハウジング	洩れ		〃	取替	4年又は、10万回
	マイクロスイッチ、水銀スイッチ	作動(設定圧力に対する)	作動不良			
	バランシングリレー	接点粗れ				
〃 モータ	ポテンショメータ	摺動部の汚れ、粗れ	作動不良 温度上昇	〃	取替	2年
〃 火炎検出器	ウルトラ球	自己放電		〃	取替	1.5年
	cds受光面	作動、抵抗	作動不良			
〃 水位制御	フロート、水銀スイッチ	作動、洩れ	作動不良	〃	交換	5年
	電極	絶縁抵抗	絶縁不良			1.5年
〃 シーケンスコントロール	リレー接点、コイル	作動 変形、変色	作動不良 温度上昇	〃	リレー取替	4年
〃 操作盤	リレー接点、コイル	作動 変形、変色	作動不良 温度上昇	〃	〃	1.5年(リレー 3年)

(3)関連法令・規格

ア．関連法令

ボイラーに関する災害を防止するために必要な事項は、産業安全及び労働衛生を統括する「労働安全衛生法」のもとで規制されている。本マニュアルで扱う機能安全の導入にあたってのリスクアセスメントを実施していく上でも、これらの関連法令や技術上の指針にしたがった設計が実施されていることが必要となる。機能安全の導入は、構造規格などの従来の安全設計基準に合致した上で、さらにそこに電気・電子・プログラマブル電子制御による安全機能を付加することで実現するものである。また、後述するリスク分析にあたっても参照すべき内容が出てくるため、対象のボイラーに関連する事項は、あらかじめ確認しておくことが必要である。

表 1-5 に主なボイラーの関連法令を列挙しておくが、下記以外の関連法令および通達などについては、http://www.jbanet.or.jp/legal/ （日本ボイラ協会）
などを参照して確認ください。

表 1-5　ボイラーの主な関連法令および通達

分類	内容
法律	労働安全衛生法
政令	労働安全衛生法施行令、労働安全衛生法関係手数料令
省令	労働安全衛生規則、 ボイラー及び圧力容器安全規則、 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、 機械等検定規則、 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の一部を改正する省令(平成 28 年厚生労働省令第 149 号)
告示	ボイラー及び第一種圧力容器製造許可基準、 ボイラー構造規格、 圧力容器構造規格、 小型ボイラー及び小型圧力容器構造規格、 簡易ボイラー等構造規格、 ボイラー技士、ボイラー溶接士及びボイラー整備士免許規程、 小型ボイラー取扱業務特別教育規程、 ボイラー取扱技能講習、化学設備関係第一種圧力容器取扱作業主任者技能講習及び普通第一種圧力容器取扱作業主任者技能講習規程、 登録性能検査機関を登録した告示、労働安全衛生法の規定により登録個別検定機関及び登録型式検定機関を登録した等の告示、

分類	内容
	ボイラー及び圧力容器安全規則第 24 条第 2 項第 4 号の規定に基づき、自動制御装置の内容を定める告示（平成 16 年厚生労働省告示第 131 号。平成 28 年厚生労働省告示第 354 号により一部改正。）
技術上の指針	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、 油炊きボイラー及びガス炊きボイラーの燃焼設備の構造及び管理に関する技術上の指針、 ボイラーの定期自主検査指針 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（平成 28 年厚生労働省告示第 353 号）
通達	ボイラーの遠隔制御監視基準等について（平成 15 年３月 31 日付け基発 0331001 号。平成 28 年９月 30 日付け基発 0930 第 35 号により一部改正。） ボイラー及び圧力容器安全規則等の一部を改正する省令の施行及びボイラー及び圧力容器安全規則第 24 条第 2 項第 4 号の規定に基づき厚生労働大臣が定める自動制御装置を定める告示の制定について（基発第 0421004 号） ボイラー等の開放検査周期に係る認定制度について（基発第 0327003 号） 「製造時等検査に係る検査の方法等」の改正について（基発 0213 第 8 号） 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の一部改正（指定外国検査機関関係を除く。）等について（平成 28 年９月 30 日付け基発 0930 第 32 号）

イ．規格

表 1-6 に、ボイラーに関する国内外の規格(参考になる関連規格を含む)を示した。これらの中で、重大な危険源とその規格上の要求事項が対比表として明記されている規格としては、JISB8407-1(ガスバーナの JIS 規格)、JISB8407-2(油バーナの JIS 規格)、JISB8415(工業炉の JIS 規格)、ISO13577-2(工業炉の燃焼設備に関する ISO 規格)があり、燃焼設備系のリスクアセスメントを実施する際には参考になる。また、安全関連システムの設計に関連する規格としては、ISO13577-4(工業炉の安全関連システム)、EN50156 シリーズ(欧州ボイラーの安全関連システム)があり、バーナコントローラの設計に関する規格としては、JISC9730-1、JISC9730-2-5(バーナコントロール)がある。ボイラーのリミッターに関する規格としては、欧州の EN12952-11、EN12952-9 が参考になる。

表 1-6　ボイラー関連規格および参考規格(ISO/IEC/JIS)

分類	規格番号/タイトル	内容
JIS	JIS B8201 陸用鋼製ボイラー構造	ボイラー構造に関する JIS 規格
JIS	JIS B8203 鋳鉄ボイラー構造	
JIS/ISO	JIS B8407-1 (ISO22967) 強制通風式バーナ 第 1 部：ガスバーナ	ISO/TC109 で制定されたガスバーナの ISO 規格
JIS/ISO	JIS B8407-2 (ISO22968) 強制通風式バーナ 第 2 部：油バーナ	ISO/TC109 で制定された油バーナの ISO 規格
JIS/IEC	JIS C9730-1(IEC60730-1)、JIS C9703-2-5(IEC60730-2-5) バーナコントロールシステム	IEC/TC72 で制定されたバーナコントロールシステムの IEC 規格
JIS	JIS B8415 工業用燃焼炉の安全通則	工業炉に関する JIS 規格
ISO	ISO13577-2　工業炉及び関連設備：燃焼及び燃料取扱システム	工業炉の燃焼設備に関する ISO 規格
ISO	ISO13577-4　工業炉及び関連設備：プロテクティブシステム	工業炉の安全関連システムに関する ISO 規格

(ア) JISB8407-1(ガスバーナの JIS 規格)、JISB8407-2(油バーナの JIS 規格)

バーナ関連の ISO 規格は ISO／TC109(Oil and gas burners)で審議され、2010 年 10 月に ISO22967:2010「Forced draught gas burners」と ISO22968:2010「Forced draught oil burners」の 2 件の ISO 規格が制定された。この ISO 規格は、欧州の EN676「automatic forced draught burners for gaseous fuels」および

EN267「automatic forced draught burners for liquid fuels」をベースに作成されたものである。

日本では、2012 年 2 月に、旧の JISB8407:2000 が廃止され、この ISO 規格に整合化した JIS B 8407-1:2012「強制通風式バーナ第 1 部：ガスバーナ」と JIS B 8407-2:2012「強制通風式バーナ第 2 部：油バーナ」の 2 部構成の規格が新たに制定され、置き換えられた。本規格は、強制通風式バーナの試験方法、構造及び運転上の一般要求事項並びに制御及び安全装置の条件について規定している。また、JIS 規格では、附属書 JA に強制通風式バーナにおいて予期し得る重大な危険源のリストが追加されており、各危険源と本文に規定されている対応防止手段の対比表が記載されている。

構造上及び運転上の要求事項を達成するための各制御機器に対しても、個別に要求事項が規定されている。この規格の対象としている機器の範囲の例は、図 1-3 の通り。

1. 手動遮断弁
2. ガス圧力計
3. フィルタ、ストレーナ
4. ガス圧力調節器
5. ガス圧力低下防止装置
6. 第 1 安全遮断弁
7. 第 2 安全遮断弁
8. 点火装置
9. 火炎検出器
10. 一次調整装置
11. 燃焼用空気流検出器
12. 空気流量低位置スイッチ
13. 稼働部安全保護部品
14. 空気流量高位置スイッチ
15. バルブ確認システム
16. 型式試験の最小範囲

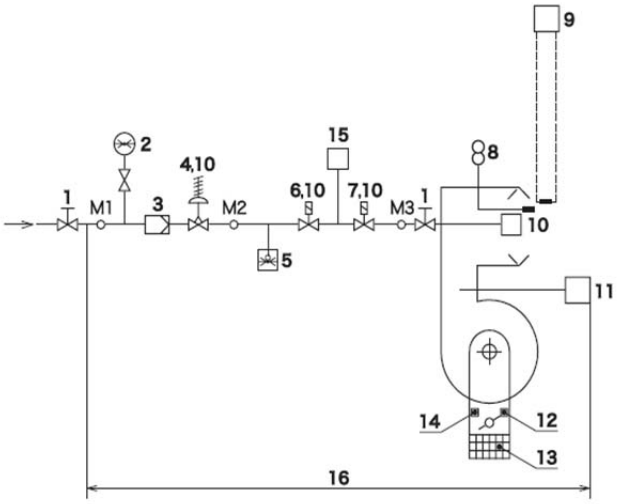


図 1-3 強制通風式ガスバーナの機器類の例

（イ）JIS C9703-2-5（バーナコントロールシステム）、JIS C9703-1(一般要求事項)

自動バーナ制御装置の国際規格としては、IEC/TC72 「Automatic electrical controls」で審議されている IEC 60730-2-5「Automatic electrical controls－Part 2-5: Particular requirements for automatic electrical burner control systems」

がある。この IEC 規格は各国で規格として採用されており、日本でも JIS C9730-2-5 として発行されている。但し、IEC 60730-2-5 は、規格改定が進んでいるが、日本の JIS は改定作業が追いついていない。日本の JIS C9730-2-5 は、IEC60730-2-5:Ed 3.1 amedment1 に基づいた規格だが、IEC の方は、Ed4.0 が発行されている。Ed4.0 では、規格のタイトルから、’for household and similar use’の部分が削除され、工業用も含めて広く他の規格から参照される規格となっている。

本規格では、機能安全に考えた方に基づいた規格要求事項が含まれており、特にシステムアーキテクチュアやソフトウエアに対する要求事項なども詳述されている。但し、JIS C9703-1(IEC60730-1　第 1 部：一般要求事項)の付属書 H に、それらの要求事項が詳述されているので、JIS C9703-1 とあわせて読む必要がある。

（ウ） ISO 13577-2(工業炉及び関連設備：燃焼及び燃料取扱いシステム)、

ISO/TC244「Industrial furnaces and associated processing equipment(工業炉及び関連処理装置)」では、工業炉の安全基準およびエネルギー効率に関する規格が審議されている。2014 年～2015 年にかけて、燃焼制御に関連する規格として ISO 13577-2、安全計装に関する規格として ISO 13577-4、各規格に使用されている用語集として ISO 13574 の合計 3 件の規格が新たに発行された。

ISO 13577-2「Industrial furnaces and associated processing equipment –safety –Part2:Combustion and fuel handling systems (工業炉及び関連設備-安全- 第 2 部 燃焼及び燃料取扱いシステム)」は、以下の範囲の安全要求事項を規定している。

・手動遮断弁とその下流側の燃料配管
・燃焼空気(酸素及び酸素富化燃焼空気を含む)及び燃焼排ガスのシステム
・バーナ、バーナシステム及び点火機器
・制御システムの安全関連部のための機能要求事項

（エ） ISO13577-4(工業炉及び関連設備：プロテクティブシステム)

ISO 13577-4「Industrial furnaces and associated processing equipment –safety-Prat4:Protective systems (工業炉及び関連設備-安全- 第 4 部：プロテクティブシステム)」は、ISO13577 の他部(第 1 部一般要求事項、第 2 部燃焼、第 3 部雰囲気ガス)で規定されている安全機能を制御システムで実行する場合、その制御システムの安全関連システムについて規定したもので、工業炉において適切な安全関連システムを構成するためのマニュアルのような規格となっている。ISO13577-4 は、機能安全のアプローチを取り入れた規定となっており、その主な内容は以下の通りである。

・安全機能を制御システムで実行する場合はプロテクティブシステムで構成する。

・プロテクティブシステムは、4 つの方法(方法 A～D)のいずれかの方法もしくはその組み合わせで構成する。

方法 A:ISO13577 他部で規定されている個別製品安全規格に適合した機器で構成

方法 B：方法 A の機器と SIL/PL に適合した機器で構成

方法 C：方法 B の機器と SIL/PL に適合した安全 PLC で構成

方法 D：機能安全規格のリスクアセスメント結果による SIL/PL 適合した機器で構成（但し火炎監視装置は個別製品規格に適合した機器が必要）

・各方法の構成例や、方法 D で実行する場合のリスクグラフによる工業炉での検討例が附属書に紹介されている。また、各機器間の接続に対しても、故障アセスメントの実施などの個別要求事項が規定されている。

（オ）欧州のボイラー関連規格

①圧力機器指令と EN 規格

図 1-4　欧州圧力機器指令と安全規格

欧州においては、ボイラーは圧力機器指令(PED、Pressure Equipment Directive)が適用される。欧州指令では、各指令に整合する欧州規格(EN 規格)が制定されており、ボイラーの場合には圧力機器指令に整合させた規格として EN12952 シリーズ(水管ボイラー)、EN12953 シリーズ(丸ボイラー)などが発行されている。例えば、EN12953 シリーズでは安全関連部は以下のような規定となっている。

・EN12953-6「Shell Boilers－Part 6: Requirements for equipment for the boiler」にて、ボイラーに使用する装置に対する要求事項が規定されている。その規定のなかで、リミッターとプロテクティブシステムが定義されている。

・リミッターとは、温度、圧力などの値が設定を超えたときに遮断し、復帰させて再起動するためには手動操作を必要とする制限機器と定義され、EN12953-9「Shell boilers － Part 9: Requirements for limiting devices of the boiler and accessories」に基づき設置し、設計しなくてはならない。

・プロテクティブシステムとは、リミッターを含む安全関連システムとされ、EN50156-1「Electrical equipment for furnaces and ancillary equipment – Part 1: Requirements for application design and installation」にしたがうことが要求されている。

②ボイラーの安全関連システムの EN 規格

EN50156-1 は 2015 年に改正され、同時に EN50156-2「Electrical equipment for furnaces and ancillary equipment Part 2:Requirements for design, development and type approval of safety devices and subsystems」が新たに発行された。EN50156-1 では、安全関連システムの基本的な設計構造を決める手順が示されており(図 1-5)、さらにこの規格で規定されている故障アセスメント手順に基づく故障解析を実施することが要求されている。この安全関連システムを構成する安全機器の設計と型式認証は、EN50156-2 により実行することが必要である。

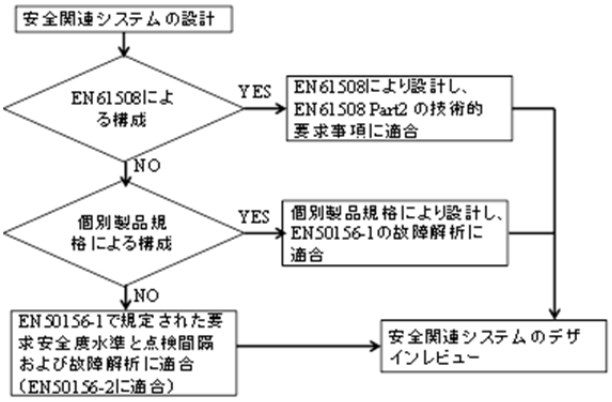


図 1-5 EN50156-1 による設計原則の選択

EN50156-2 では、安全機器の設計と型式認証について、個別機器の EN 規格にしたがう方法と、個別機器の EN 規格ではなく機能安全にしたがう方法の二つが示されている。電気/電子/プログラマブル電子システムの安全機器の場合には以下の通りである。

a)個別製品規格による型式認証(電気/電子/プログラマブル電子システムの機器およびサブシステム)

次の製品規格に基づき試験された機器を使用する。

EN 298:2012 (バーナコントロール), EN 1643:2014(バルブプルービングシステム), EN 1854:2010(ガス/エア圧力検出器), EN 12952-11:2007(水管ボイラーのリミット機器), EN 12953-9:2007(シェルボイラーのリミット機器) , EN12067-2:2004(空燃比制御電気式), EN 13611:2007+A2:2011(バーナ制御機器一般要求事項), EN 16340:2014(排ガス検出器), EN ISO 23552-1:2014(空燃比制御電気式),

また、この場合、装置規格の安全要求事項(例えば水管ボイラーなら EN 12952 シリーズの関連事項)も考慮しなくてはならない。

b)EN61508 による型式認証

機能安全に基づく型式認証となり、EN61508 シリーズ全てに適合しなくてはならない。さらに、環境及び電気安全は、EN 61131-2:2007, EN 60730-1:2011, EN 61010-1:2010.のいずれかの要求事項に対応することが必要となる。

この他、安全関連システム内の電気システムに接続される機械式、液圧、空圧機器はその他の技術の機器と定義されて、これについても以下の二つの方法が示されている。

c)個別製品規格による型式認証(機械式、液圧、空圧機器、その他)

次の製品規格に基づき試験された機器を使用する。

EN 161:2011+A3:2013(ガス自動遮断弁), EN 267:2009+A1:2011(強制通風式オイルバーナ), EN 676:2003+A2:2008(強制通風式ガスバーナ), EN 1854:2010(ガス/エア圧力検出器),EN ISO 23553-1:2014(オイル自動/半自動弁), EN12952-11:2007(水管ボイラのリミット機器), EN 12953-9:2007(シェルボイラのリミット機器), EN 13611:2007+A2:2011(バーナ制御機器一般要求事項), EN 60947-2:2006 (回路遮断器/配線用ブレーカ)

d)故障アセスメントによる型式認証(機械式、液圧、空圧機器、その他)

上記③で示した各製品規格にはないその他の機器については、EN50156-1 で示されている故障アセスメントと、EN 60812:2006 による FMEA による方法を組み合わせて評価する必要がある。この場合も可能な限り製品規格の安全要求事項を考慮しなくてはならない。また、環境及び電気安全は、EN 61131-2:2007, EN 60730-1:2011, EN 61010-1:2010.のいずれかの要求事項に対応することが必要となる。

2. ボイラー制御系と安全関連システムの区分

機能安全の導入にあたってはボイラーの制御部を、通常の制御システムと安全関連システムに分けて設計しなくてはならない(図 1-6)。

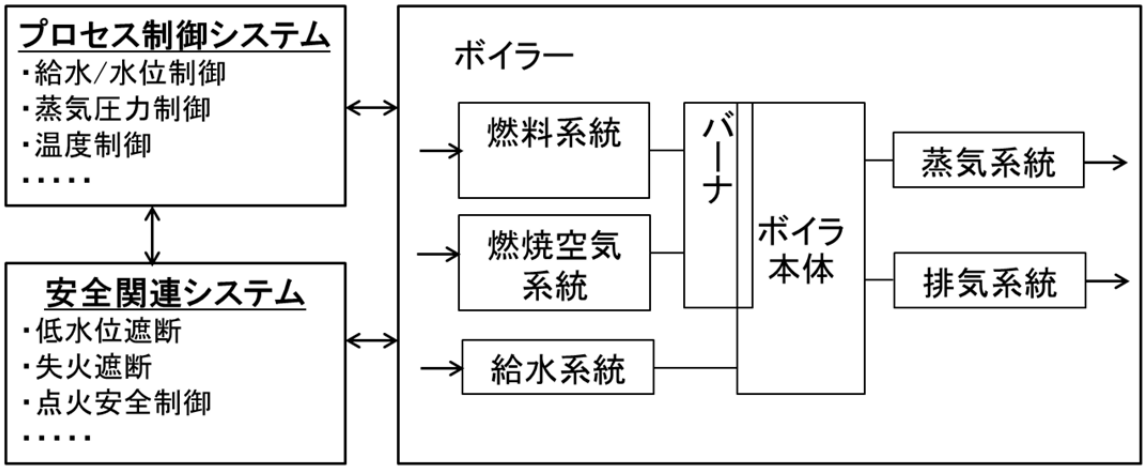


図 1-6 ボイラー制御システムと安全関連システム

これは、通常の制御システムの故障が直接安全関連システムの機能に影響を与えることを、最小限に抑えることが必要なためである

水位制御を例にすると、図 1-7 のようになる。この例では、水位レベルを差圧発信器で調節計へ入力して給水調節弁で給水量を制御し、これとは別系統で低水位検出用としてフロートスイッチを使用して燃料遮断弁を閉じる構成としている。燃料遮断弁は、低水位検出の確認信号と、運転信号の AND で制御される。

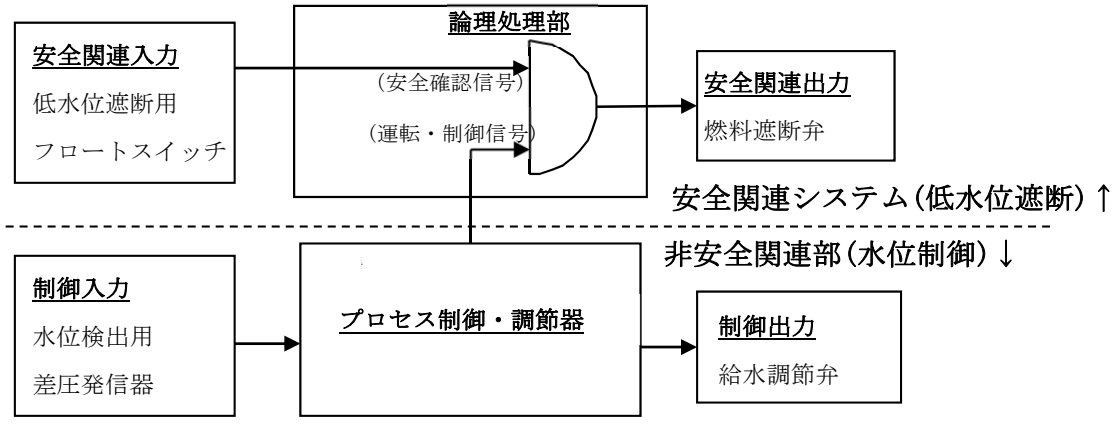


図 1-7 水位制御と低水位遮断機能の構成例

これに比較して、図 1-8 は、安全関連システムとの分離が不十分な例である。図 1-8 では、低水位検出の信号を通常の制御系システムで生成した信号からとって構成しており、この構成の場合には、通常の制御系システムの故障も加味して安全関連システムの設計が必要となってしまう。したがって、通常の制御系も安全関連システムとして設計しなくてはならなくなる。

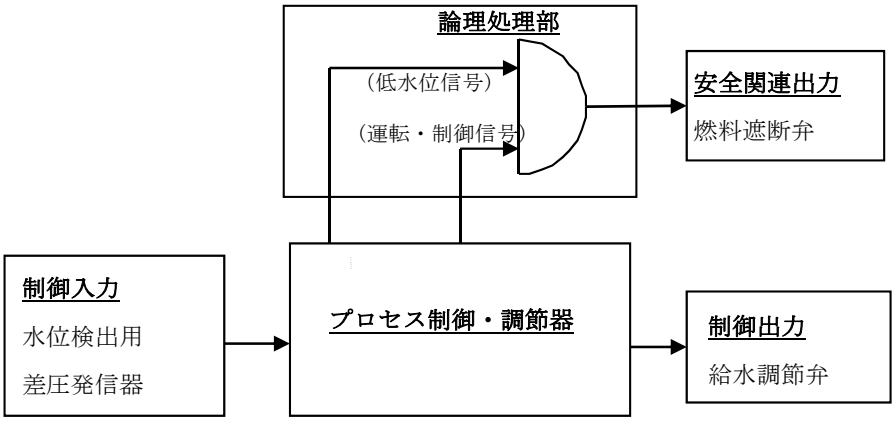


図　1-8　水位制御と低水位遮断機能の分離が不明瞭な例

第２章ボイラー制御系のリスクアセスメント（リスク分析）、要求安全機能の特定、要求安全度水準の決定

1. リスク分析

第１章で決定したリスクアセスメント範囲、仕様、使用条件を基にして、故障モード影響分析（FMEA）やフォールトツリー解析（FTA)、ハザード・オペレーション分析（HAZOP）等の手法を使用してリスク分析を実施する。リスク分析にあたっては、予見可能な誤使用（ヒューマンエラー）を含めて実施し、また、少なくとも、「ボイラーの遠隔制御監視基準等について(基発第 0331001 号)」に規定されている以下の重故障の内容を含めて実施することが必要である。

・ボイラーの圧力の異常上昇
・ボイラーの水位の異常低下
・バーナの異常消火
・操作用動力源の喪失
・通風機の停止
・燃料圧力の異常低下
・燃料圧力の異常上昇

(1)FTA 実施例(水位の異常低下)

図 1-7 で説明した水位制御と低水位遮断を例として、FTA を実施する場合、以下のような手順となる。

ア．機能ブロック図の作成

図 1-7 で示したように、ボイラーの水位制御系は、非安全関連部(給水制御系)と安全関連システム(低水位遮断系)に分けられる。ここでの FTA を実施する目的は、給水制御系が水位の異常低下を引き起す要因を分析することである。FTA で抽出した要因を基にして、次章で安全関連システム(低水位遮断系)に要求される安全度水準を設計していくことになる。したがって、まずは給水制御系の機能ブロック図を作成する。

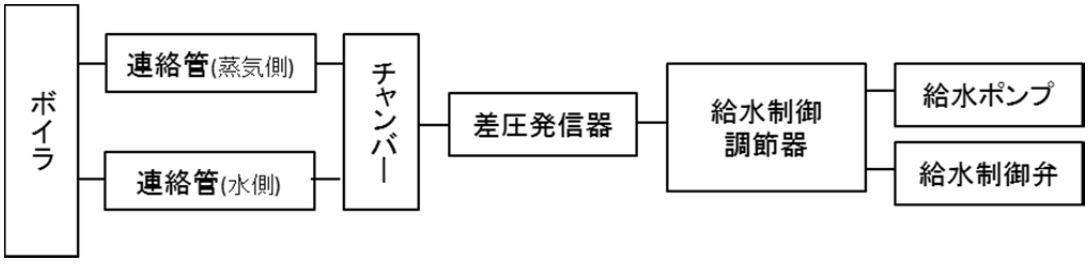


図　2-1 給水制御系の機能ブロック図例

機能ブロック図の中の機能単位は、故障解析に必要となるおおよその機能単位で作成する。例えば、図 2-1 では、ロジック処理部分を給水制御・調節器としているが、この部分の回路は、液面調節器やシーケンス制御部などの機能ブロックにさらに分解可能であるが、ここではロジック処理部分を一つの機能ブロックとしてまとめて記述している。

イ．FTA 図の作成

機能ブロック図を参考にして FTA を実施する。ここで使用する FTA 図は、トップ事象を発生させる原因または原因の組合せを明確化することが目的である。ここで明確化された原因を基にして、要求安全機能を特定する解析を実施することになる。トップ事象には、危険事象として前項に記載した重故障をおき解析を進める。図 2-1 の機能ブロック図をもとにした実施した FTA 図の例を図 2-2 に示す。

ここでは対象のボイラーを炉筒煙管ボイラーとしているので、トップ事象は水位の異常低下による炉筒圧壊と記述されている。同じ水位の異常低下であっても、ボイラー構造の差異などにより危険事象が必ずしも同じになるとは限らない。例えば、ボイラーによっては、水位の異常低下による異常高温(排気系など)での火災がトップ事象になることもある。

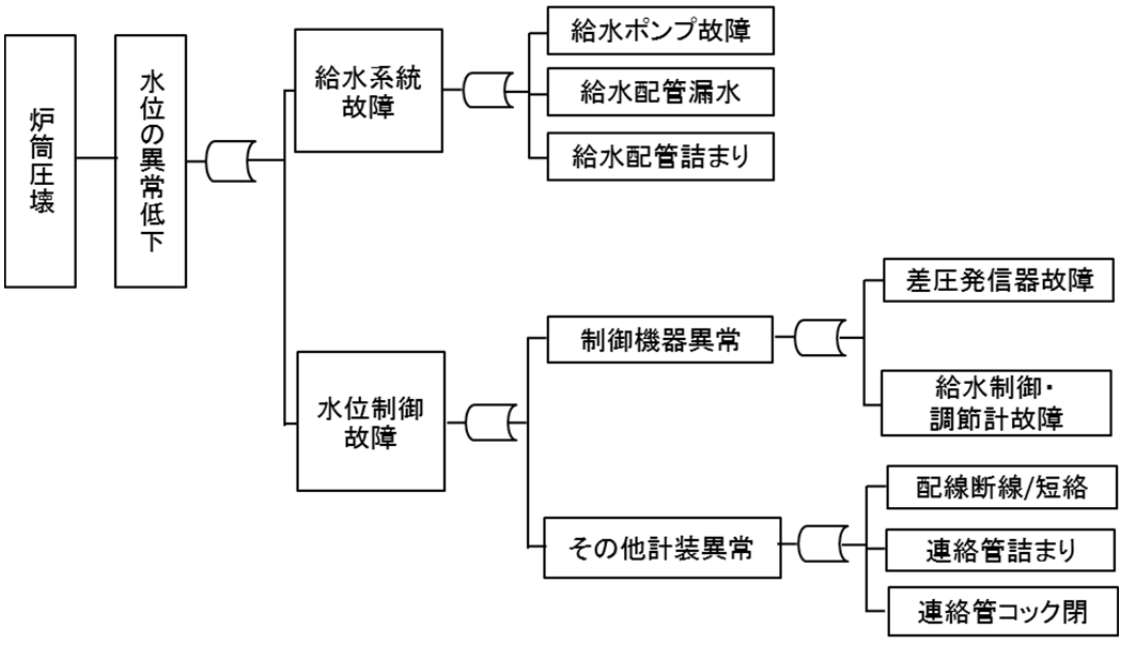


図 2-2 炉筒煙管ボイラーの FTA 図例(水位の異常低下)

(2)FTA 実施例（バーナ異常失火）

図 1-2 で示した自動制御系統図のガスバーナ制御系統を例として、FTA を実施する場合、以下のような手順となる。(バーナ周辺部分を図 2-3 に示す)

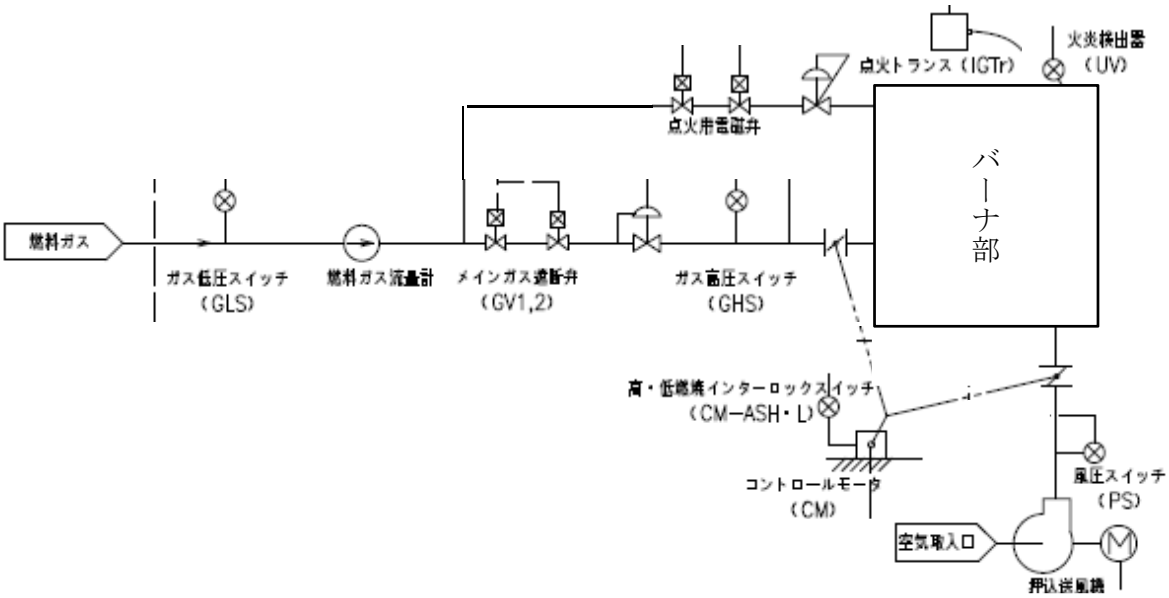


図 2-3 ガスバーナ制御系統の例(図 1-2 より抜粋)

ア．機能ブロック図/FTA 図の作成

ここでは、前項に記載した重故障のうち「バーナの異常消火」による危険事象として、FTA のトップ事象をガス燃料による爆発とする。ガス燃料を流出/滞留させる要因としては、「バーナの異常失火」の他にも、「ガス配管系統からの漏れ」「ガス遮断弁の故障」などの項目があるので、それらを全て書き出して、FTA 図の作成を開始する。その際、必要に応じて検討項目に対応する機能ブロック図を準備して実施する(図 2-4)。

例えば、図 2-5 では「バーナの異常失火」に対する要因の一つとして「空気量不足/過多」を上げており、これに関連する制御は燃焼量制御であり、この機能ブロック図を確認した上で、図 2-6 のようにさらに FTA を進めている。どこまで詳細な要因まで検討を進めるかの目安としては、構成する機器や構造部品もしくは作業項目が抽出されるまで進めることが必要である。

なお、この例では、バーナの異常失火により未燃ガスが発生してしまう要因を検討しているため、例えばガス遮断弁が誤作動してガス遮断してしまい、その結果として異常失火してしまうような要因(ガスが誤って遮断されることにより異常失火となる要因)は記載していない。

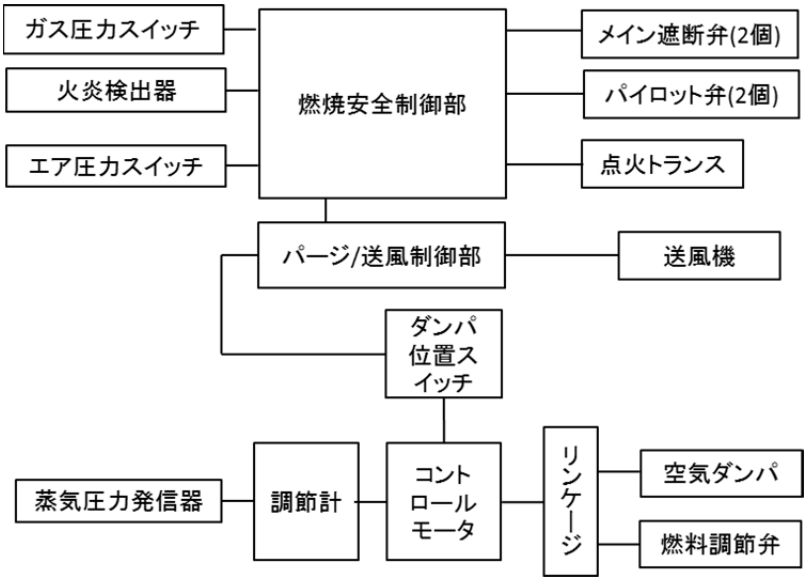


図　2-4 燃焼制御系機能ブロック図例

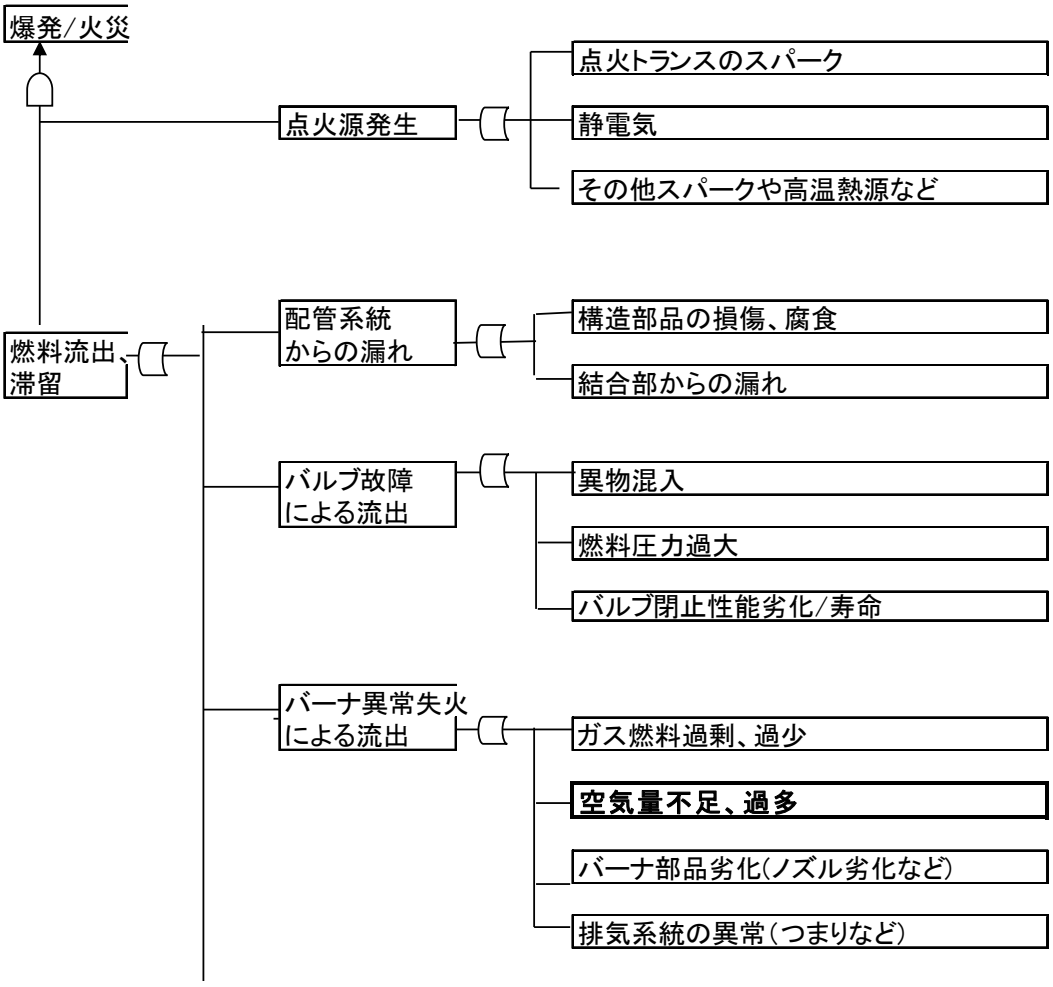


図　2-5 炉筒煙管ボイラーの爆発火災 FTA 図例

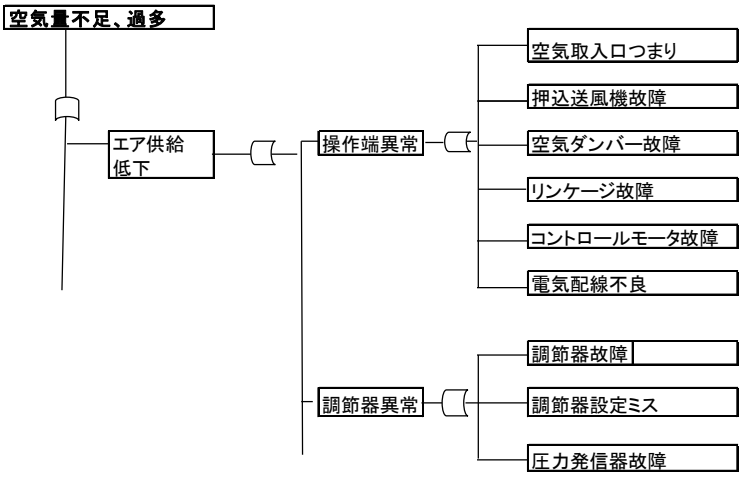


図 2-6 バーナ空気量不足の FTA 図例

イ．燃焼系統の FTA の留意点

図 2-5、図 2-6 では、炉筒煙管ボイラーでのガスバーナを使用した例を記載しているが、燃焼系統の FTA では燃料の種類とバーナ特性などによって危険事象やリスク要因が異なってくる。例えば、油燃焼の場合には、燃料温度、油中の水分・スラッジ、噴霧媒体系の異常なども検討の管理対象となる。

ウ．バイオマスボイラーの事例

バイオマスボイラーの事例を図 2-7 に示す。図 2-7 のバイオマス温水ボイラーでは、一次、二次と 2 段に分けて燃焼空気を供給し燃焼ガスが熱交換部へ供給される。その後誘引ファンにより排気されるが、排気も再循環させて、燃焼制御している。排気系統には O2 センサと温度センサが設置されている。また、熱交換部には冷却水系統があり、余剰熱を放熱し缶水温度の上昇を抑制している。冷却しても缶水温度の異常高温が継続した場合には、燃料供給を停止する機能がある。

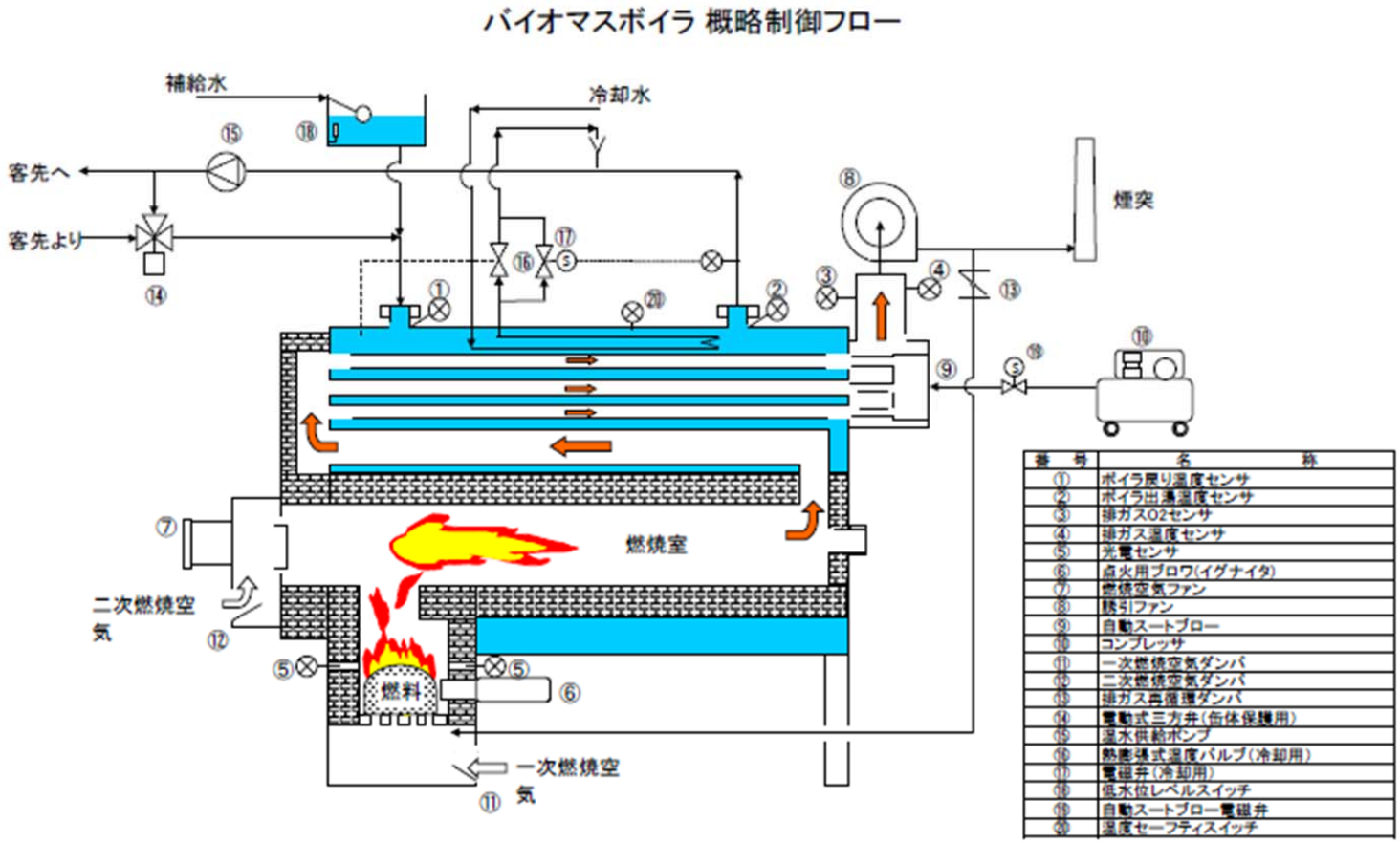
通常の停止動作では、排ガス酸素濃度が上昇し、かつ排ガス温度が低下したところで、燃焼停止(燃焼ガスの発生停止)したと判断し、排気ファン、循環ファンを停止する。その間、温水ポンプは運転継続し、内部循環して缶体を保護している。温水温度が十分に低下したところで、温水ポンプも停止し、ボイラー運転停止となる。

図 2-8、図 2-9 に FTA 図 の例を示す。燃焼系統については、危険事象として爆発または CO 大量発生をトップ事象として解析をすすめており、その原因としては、排気系統の異常による炉内圧上昇、空気量不足・燃料過多による不完全燃焼などがある。給水系統については、危険事象として空焚きによる火災をトップ事象とし、缶水量異常低下と冷却機能低下の両方が発生した場合に空焚き状態となるとしている。缶水量異常低下の原因としては補給水不足または循環量低下という現象があり、それぞれの

現象について解析を進めている。また、冷却機能低下の原因としては、冷却水配管漏れ/詰まり、制御機器の動作不良などがある。

この給水系統の FTA の例のように、危険事象を引き起こす一次要因の現象に分けてから、FTA を進めることは、漏れなく原因を抽出するためには有効な方法である。また、ボイラーの運転状況によって故障の影響が異なってくることが想定される場合には、ボイラー運転開始時、ボイラー定常運転中、ボイラー停止動作中などとボイラーのシーケンス毎に解析を進めることも必要である。

図　2-7　バイオマスボイラーの例



番　号	名　　称
①	ボイラ戻り温度センサ
②	ボイラ出湯温度センサ
③	排ガスO2センサ
④	排ガス温度センサ
⑤	光電センサ
⑥	点火用ブロワ(イグナイタ)
⑦	燃焼空気ファン
⑧	誘引ファン
⑨	自動スートブロー
⑩	コンプレッサ
⑪	一次燃焼空気ダンパ
⑫	二次燃焼空気ダンパ
⑬	排ガス再循環ダンパ
⑭	電動式三方弁(缶体保護用)
⑮	温水供給ポンプ
⑯	熱膨張式温度バルブ(冷却用)
⑰	電磁弁(冷却用)
⑱	低水位レベルスイッチ
⑲	自動スートブロー電磁弁
⑳	温度セーフティスイッチ

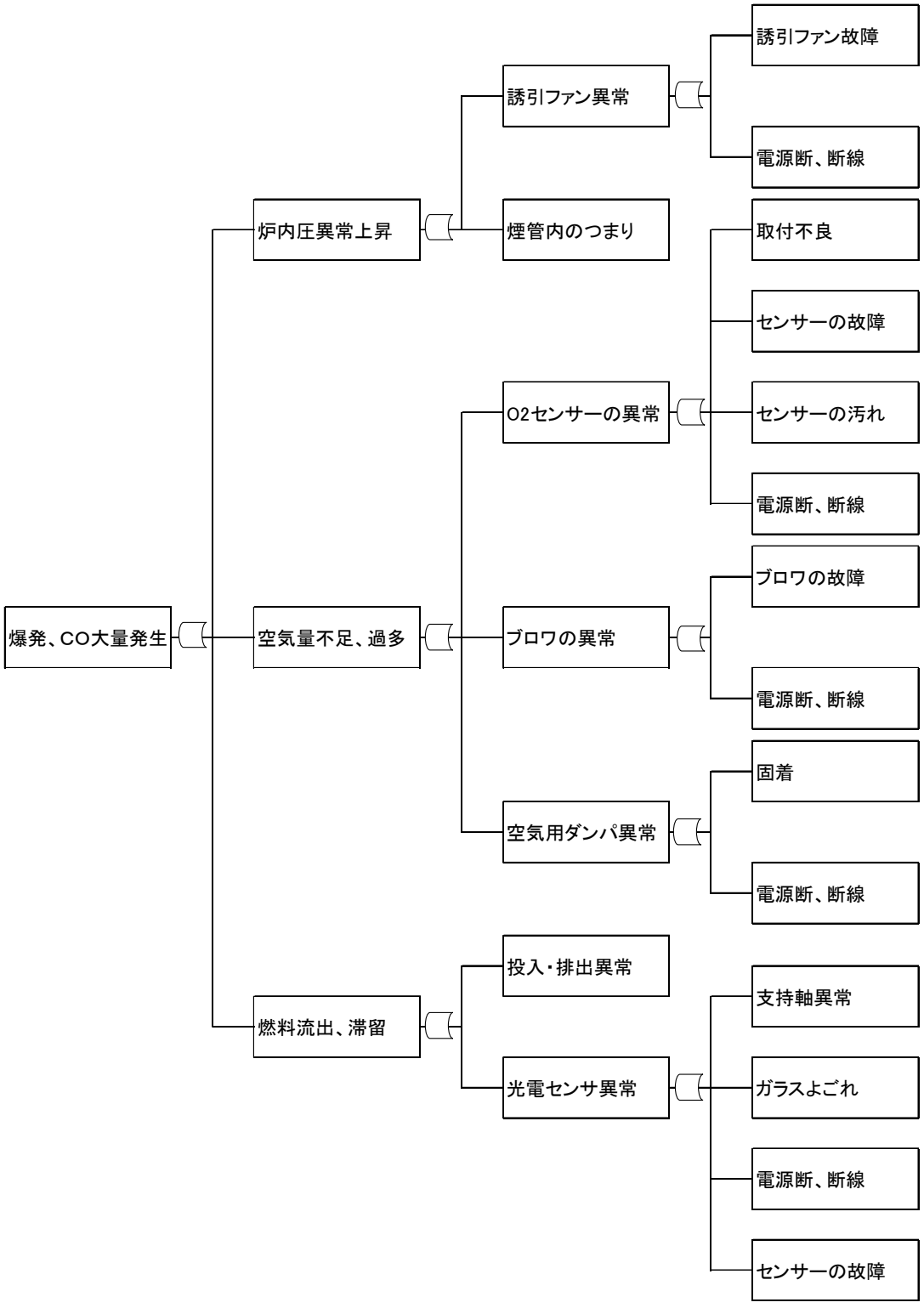


図　2-8 バイオマスボイラーの燃焼系 FTA 図例

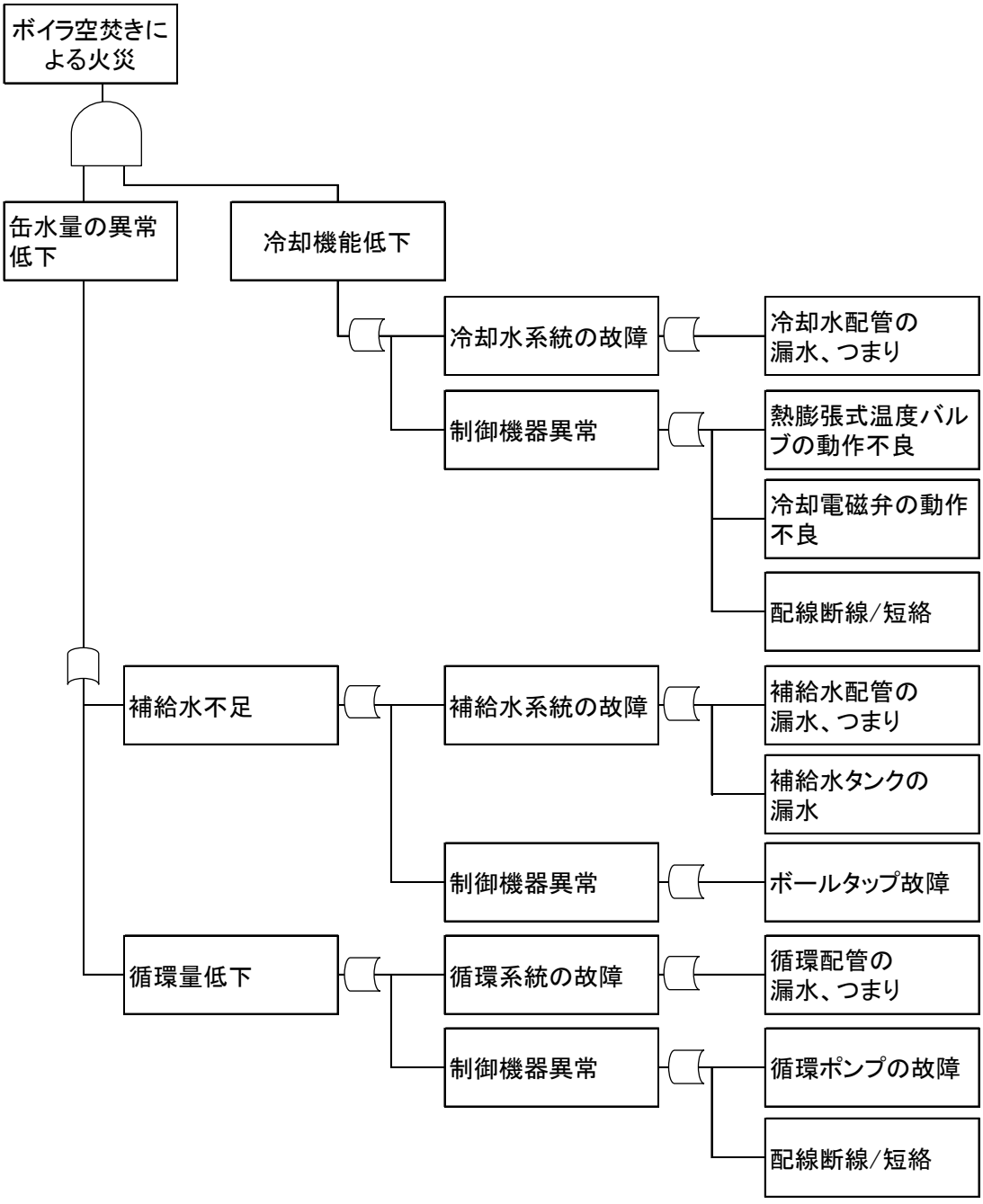


図 2-9 バイオマスボイラーの給水系 FTA 図例

2. 要求安全機能の特定、要求安全度水準の決定、使用者への情報

次に、前項で実施したFTAなどによるリスク解析の結果に基づき、要求される安全機能を特定し、その安全機能に必要となる安全度水準を決定し、使用者への情報を決定する。ここまでの内容が決まれば、このシステムに要求される安全要求仕様が決定したことになる。

本マニュアルでは、要求安全機能の特定、安全度水準の決定、使用者への情報は、表2-1を使用した方法を説明する。

(1)要求安全機能の特定

ア.表 2-1 の使い方

要求安全機能を特定する際には「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」の欄に内容を記入する。

キーワード：FTAで実施した解析の概要を示す内容

危険側故障：FTAで抽出した危険側故障の内容

危険事象：労働者などの人に負傷または疾病を生じさせる事象を記入

(危険事象は同じ異常状態であっても、ボイラー種類によって異なる場合があるので注意が必要である。例えば、水位の異常低下で空炊きになると、炉筒煙管ボイラーなら圧壊に至る可能性があるが、貫流ボイラーなら排気温度が高温となり火災に至る可能性がある)

検出方法：故障を検出する方法を記入。

(FTA を使用した場合、抽出した危険側故障からトップ事象の危険事象に至る経路のどこかで検出する方策を検討することが必要となる)

要求安全機能：電気・電子・プログラマブル制御にて要求される安全機能を記入。

記入する際には、入力/ロジック/出力が明確になる表現で記述しておくことが望ましい。

作動要求に関する事項：故障内容及び要求安全機能に関連する構造上の要件や機械式安全装置(安全弁など)を記入。

イ.水位の異常低下での例

図2-2の水位の異常低下のFTA図を例にすると以下のようになる。

キーワード：

重故障のひとつである水位の異常低下をキーワードとする。

危険側故障：

FTA図の最下段の内容を記載、例えば「連絡管つまり、連絡管コック閉」。

危険事象：

トップ事象である「炉筒圧壊」

検出方法：

トップ事象のひとつ下の水位の異常低下を低水位検出器で検出。

要求安全機能：

水位が安全低水面以下になった場合に燃料を遮断(低水位遮断)と記入

作動要求に関する事項：

「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」の構造要求に適合と記入。特に「連絡管コック閉」に対しては、連絡管は他の水位検出器の連絡管と分離することが構造上要求されることを記入。

(2)安全度水準の決定

要求安全機能が特定されたら、次にその安全機能に要求される安全度水準を決定する。安全度水準の決定方法には、リスクグラフ法による方法(IEC61508-5 付属書 D、ISO13849-1 付属書 A)とマトリクス法(IEC62061 付属書 A)がある。本マニュアルでは、リスクグラフ法による事例を説明する。

ア.表 2-1 の使い方

安全度水準を決定する際には「要求安全度水準」の欄に各パラメータ値を記入し SIL 数値を決定

C: 負傷又は疾病の重篤度(C_A, C_B, C_C, C_D)

F：危険性又は有害性へのばく露頻度(F_A, F_B)

P：危険事象の回避可能性(P_A, P_B)

W：要求安全機能の作動要求確率(W_1, W_2, W_3)

SIL：要求安全度水準(1, 2, 3, 4)、その他(-, a, b)

イ.各パラメータの決定方法

図 2-10 に基づき各安全機能ごとに評価して安全度水準を決定する。各評価パラメータの評価結果とそれにより決定した要求安全度水準を表 2-1 に記載する。各評価項目についての判断基準は以下の通りである。

・負傷又は疾病の重篤度(C)

第 1 章 1-(2)-イ（7 ページ）に記載した使用条件の設置場所/設置環境に基づき重篤度を判断する。7 ページにも記載したように、通常のボイラー設置環境にて、ボイラーの爆発/火災が発生した場合の重篤度は複数死亡(Cd)と評価する。特別に隔離された環境での使用などの特別な条件が規定される場合に限って、ボイラーの爆発/火災に対する重篤度を Cc 以下の重篤度とすることができる。

・危険性又は有害性へのばく露頻度(F)

第 1 章 1-(2)-イ（7 ページ）に記載した使用条件に基づき、ばく露頻度を判断する。運転条件が 12 時間以下なら、その他の使用条件に関わらず F_A(1 日 12 時間以下)となる。運転条件が 12 時間を超える場合には、その他の使用条件(人がどの程度の頻度でボイラー運転中にボイラー設置場所周辺にいるのか)を加味して、F_B(1 日 12 時間超)とするかどうか判断する。

・危険事象の回避可能性(P)

一定程度回避可能かどうかは、その危険事象の進展速度(突発か徐々にか)、その危険事象のプロセスが監視されているか、危険の認識の容易性(異常を直ちに見ることができるか)、危険事象からの回避性(待避路があるか)などから総合的に判断する。例えば、ボイラーの爆発では、突発的に進展する可能性があるため回避不可能と判断することが妥当であるが、もし一定程度回避可能とするなら、その条件を明確にしておく必要がある。また、火災の場合には、消防法等に基づく対応などが実施されているので、回避可能と判断しても差し支えない。

・要求安全機能の作動要求確率(W)

これは、この安全関連系がない状態で、その他の外的リスク軽減施策を含む状態で、その事象が起きる頻度を推定することである。ボイラーの場合には、すでに既存の各種リスク軽減策が法令上の要求を含めて実施されている状態にあるので、要求安全機能の作動要求確率は、W1(非常に低い)と判断して良い。但し、法令上などの要求にない特殊な安全機能が要求されている場合には、外的リスク軽減策が実施されるのかどうか確認して判断する必要がある。

・要求安全度水準(SIL)

上記した 4 つのパラメータ、負傷又は疾病の重篤度(C_A, C_B, C_C, C_D)、危険性又は有害性へのばく露頻度(F_A, F_B)、危険事象の回避可能性(P_A, P_B)、要求安全機能の作動要求確率(W1,W2,W3)を図 2-10 あてはめて、要求安全度水準(1,2,3,4)、その他(-,a,b)を決定する。

(3)使用者への情報

使用者への情報を決定する際には、「製造者追加対策」、「使用者追加対策」の欄に内容を記入する。この使用者への情報で記載される事項は、プルーフテスト間隔を決定する設計条件としても参照されることになる。

・製造者追加対策

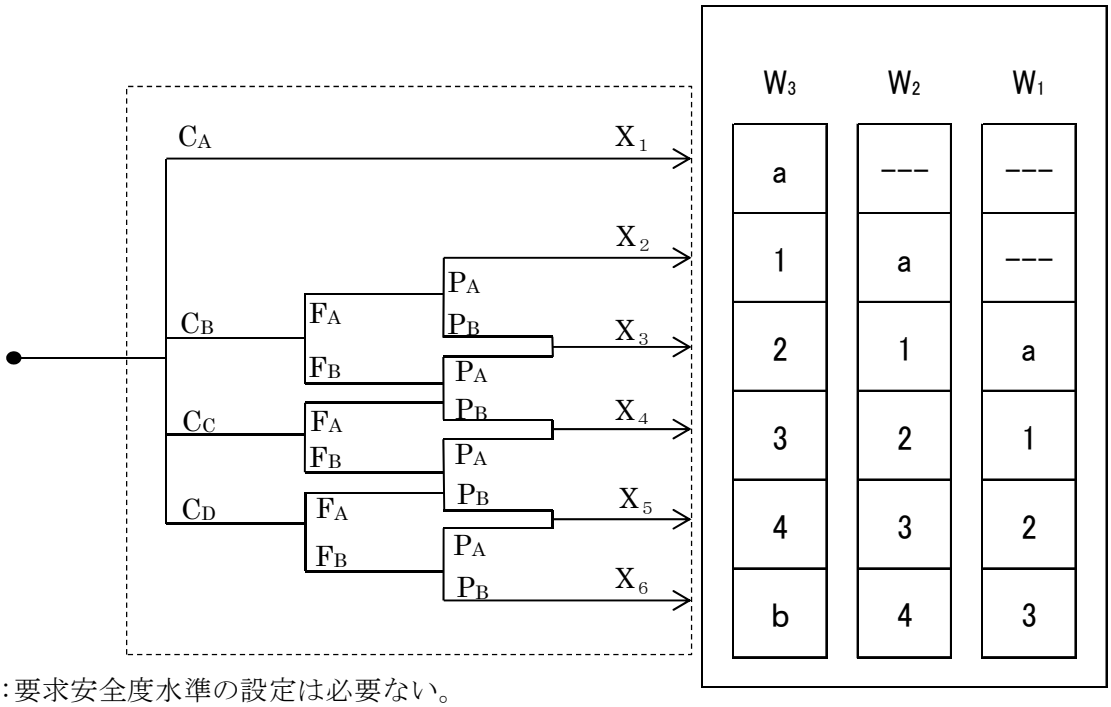
取扱説明書記載事項、点検内容に関連して、製造者側で必要となる対策を記入する。

例：連絡管は内部掃除が容易な構造とする。

・使用者追加対策

取扱説明書記載事項、点検内容に関して、使用者にて特に留意すべき対策を記入。

例：給水圧力、水面計、水位制御機能の日常点検。コックの開閉状態の確認。



a:要求安全度水準の設定は必要ない。

b:単一の安全関連システムでは要求安全度水準を達成することはできない。

負傷又は疾病の重篤度(C)		危険性又は有害性へのばく露頻度(F)		危険事象の回避可能性(P)		要求安全機能の作動要求確率(W)	
C_A	軽傷	F_A	1 日 12 時間以下	P_A	一定程度可能	W_1	非常に低い
C_B	後遺障害	F_B	1 日 12 時間超	P_B	困難	W_2	低い
C_C	死亡					W_3	高い
C_D	複数死亡						

図 2-10 リスクグラフ法による要求安全度の決定

表 2-1 要求安全機能の特定/安全度水準の決定/使用者への情報

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	給水系統の配管,機器からの漏れの日常点検
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

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
7	異常失火	空気取入れ口詰まり	空気量不足による異常失火で爆発	火炎検出器	失火を検出した場合には燃料を遮断	燃焼用空気の風道は、空気の流れを確保するため、その損壊、地下水の浸入等が生じない構造のものとする	C_D	F_A	P_B	W_1	2	エアフィルタ等の設置、 火炎監視窓の設置、	空気取入れ口の日常点検、燃焼音・火炎の色・形状の確認、排ガス分析、
8	異常失火	送風機故障	空気量不足による異常失火で爆発	火炎検出器	失火を検出した場合には燃料を遮断	送風機モータへの通電がなくなれば直ちに燃料遮断する構成とする。	C_D	F_A	P_B	W_1	2	No7 と同じ	送風機の日常点検、燃焼音・火炎の色・形状の確認、排ガス分析
9	燃料流出	遮断弁越しのガス漏れ(異物混入他)	ガス燃料流出による爆発	遮断弁閉確認スイッチ	バーナ起動時に遮断弁閉確認できない場合には停止	ガス遮断弁は直列に 2 個設置すること。	C_D	F_A	P_B	W_1	2	-	弁、フランジ、ガス配管の漏れ点検、
10	燃料流出	寿命による弁閉止性能の劣化	ガス燃料流出による爆発	遮断弁閉確認スイッチ	バーナ起動時に遮断弁閉確認できない場合には停止	ガス遮断弁は直列に 2 個設置すること。	C_D	F_A	P_B	W_1	2	-	弁、フランジ、ガス配管の漏れ点検
11	不完全燃焼	空気取入れ口詰まり	不完全燃焼で CO 大量発生	圧力スイッチ	エア圧力が設定値より低下した場合には燃料を遮断	No7 と同じ	C_D	F_A	P_B	W_1	2	No7 と同じ	No7 と同じ、 圧力スイッチの設定値、導管のつまり漏れ確認

第３章 要求安全度水準に適合する設計（システム設計）

１　はじめに

本章では、ボイラーの安全関連システムの事例をもとにして安全度水準（SIL）の評価について示す。安全関連システムの安全度水準（SIL）が要求安全度に適合することを示すためには、安全関連システムを構成する製品の SIL の評価とともに、全体システムの SIL の評価が必要になる。２.２では、製品レベルとシステムレベルの SIL の評価の流れや条件設定の具体的な方法、PFDavg の計算方法について示し、２.３でボイラーのシステム設計の具体例をもとにして SIL の評価を実施する。

２　SIL の評価フロー

安全関連システムを構成する製品の SIL を求める評価フローを図１に示し、システムの SIL を求める評価フローを図２に示す

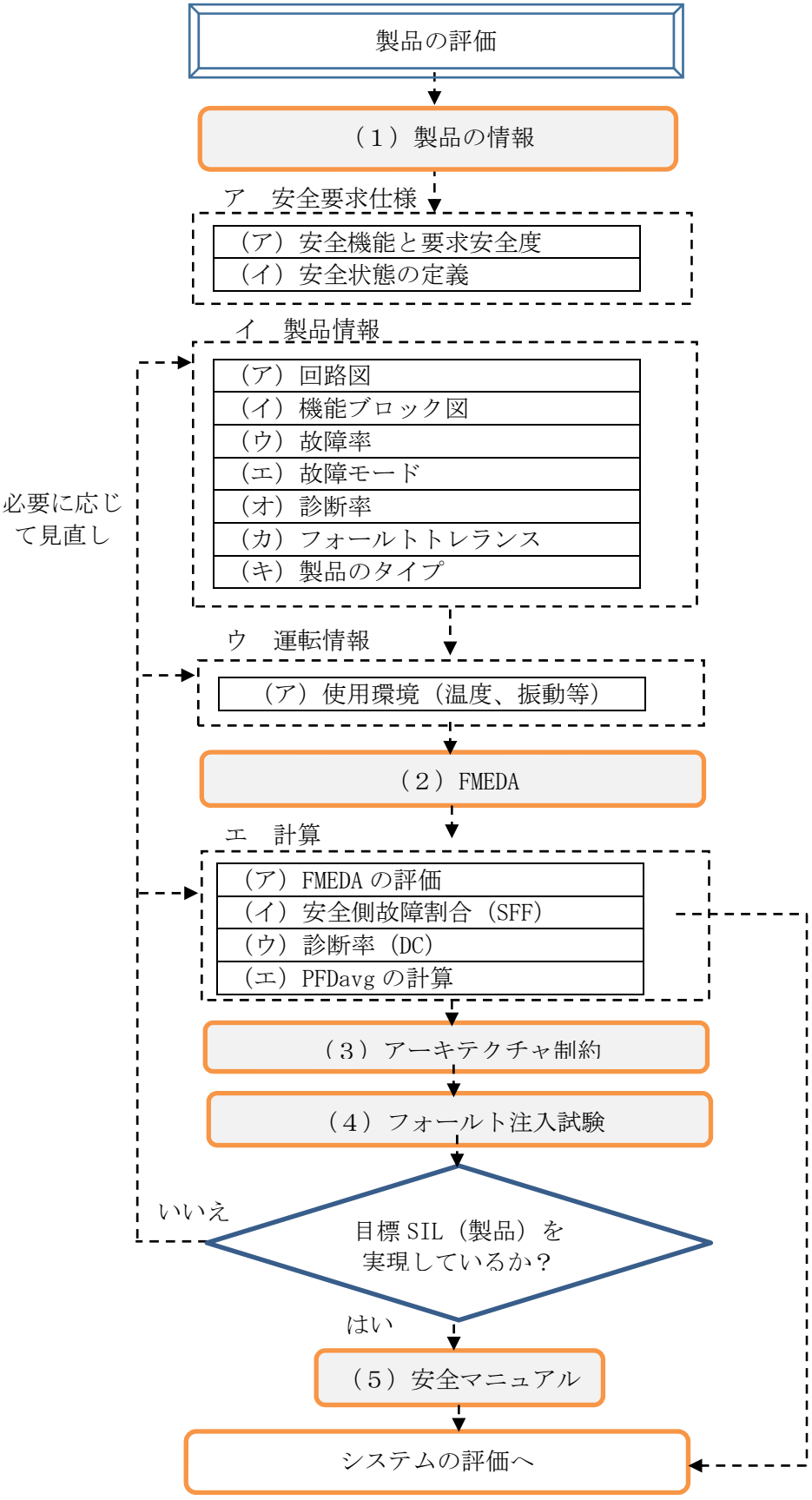


図１　製品の SIL の評価フロー

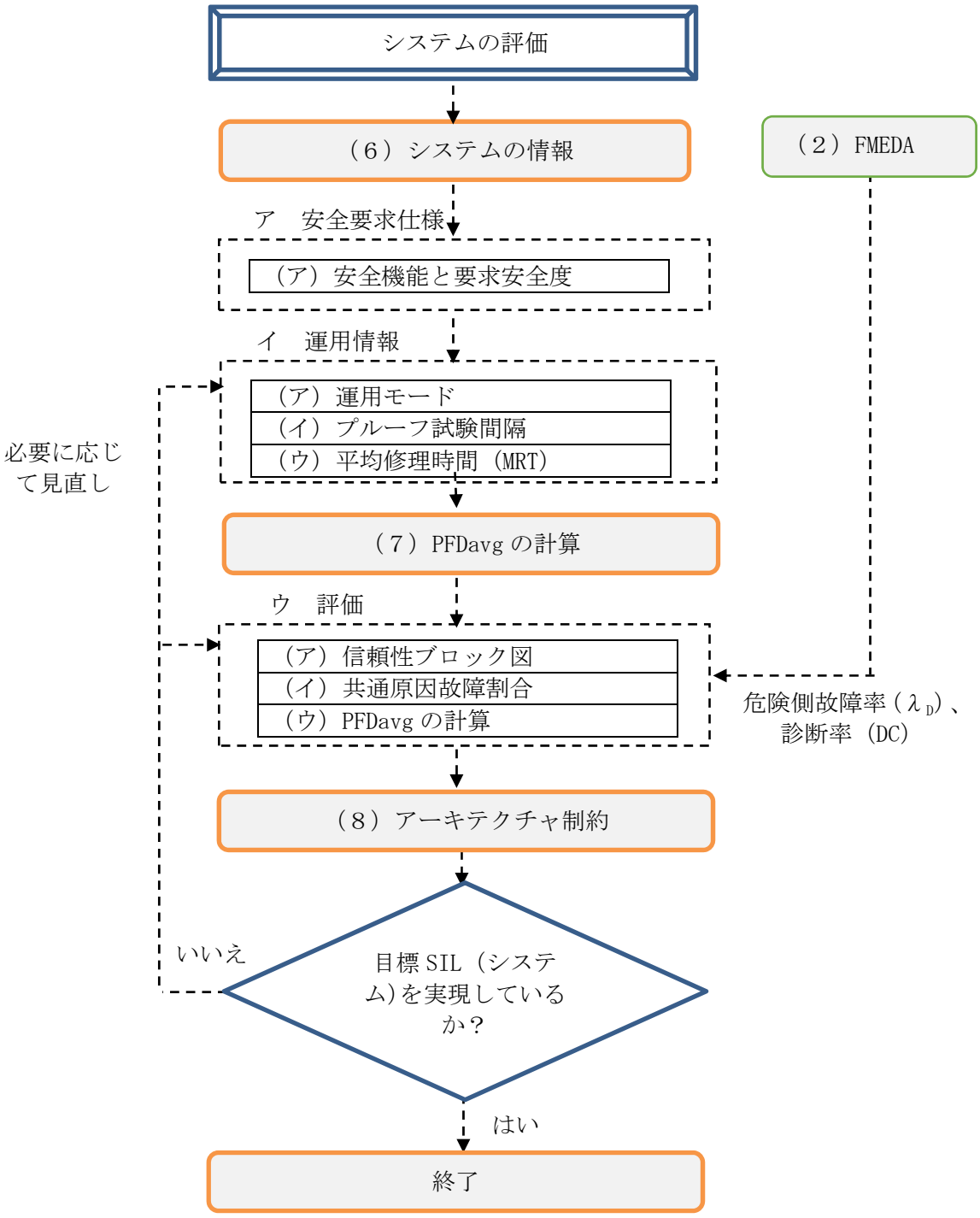


図２　システムの SIL の評価フロー

SIL を評価するためには、次の要求事項を同時に満たす必要がある。
・ランダムハードウェア故障確率
・アーキテクチャ制約

また、両者は、製品レベルとシステムレベルで評価を行う必要があり、それぞれ、2.1 製品の評価と 2,2 システムの評価において解説する。

２．１　製品の評価

最初に製品レベルで FMEDA を実施する必要がある。ただし、製品が認証されている場合で FMEDA の結果を入手でき、かつ、評価条件に問題がなければ、あらためて評価をする必要はない。認証製品を使用しない場合には、部品の故障率や故障モード等のデータをもとにして FMEDA によって製品の分析を行う。

図１に従って製品の評価を行う上での情報の入手や評価方法について以下に解説する。

（１）製品の情報

ア　安全要求仕様

（ア） 安全機能と要求安全度

安全要求仕様書から評価の対象となる安全機能と要求安全度を識別する。IEC 61508 第 4 部 3.5.1 には次のような安全機能の事例がある。

＊ 危険な状況を回避する積極的な動作として実行することが要求される機能(例えば、モーターのスイッチ切断);
＊ とられている動作を妨げる機能(例えば、モーター起動の防止)。

安全機能の目的も合わせて明確に記述し、複数の安全機能があれば網羅することが必要である。

（イ） 安全状態の定義

IEC 61508 第 4 部 3.5.1 には安全な状態とは、「安全が達成される場合の EUC の状態」とあるが、この状態が明確に定義されていないと、FMEDA を実施する場合に一貫性がなくなるので、考慮すべき安全状態を明確に定義する。

イ　製品情報

（ア） 回路図

安全関連システムを構成する製品の部品リストや回路図が必要である。制御系と安全関連システムの一部が混在するような回路図には、あらかじめ、安全系と非安全系の区分けを行い、かつ、構成要素の名称（電源部、入力部、出力部など）を回路図上に記入し、後の機能ブロック図の作成に使用する。回路図の記入事例を図３に示す。

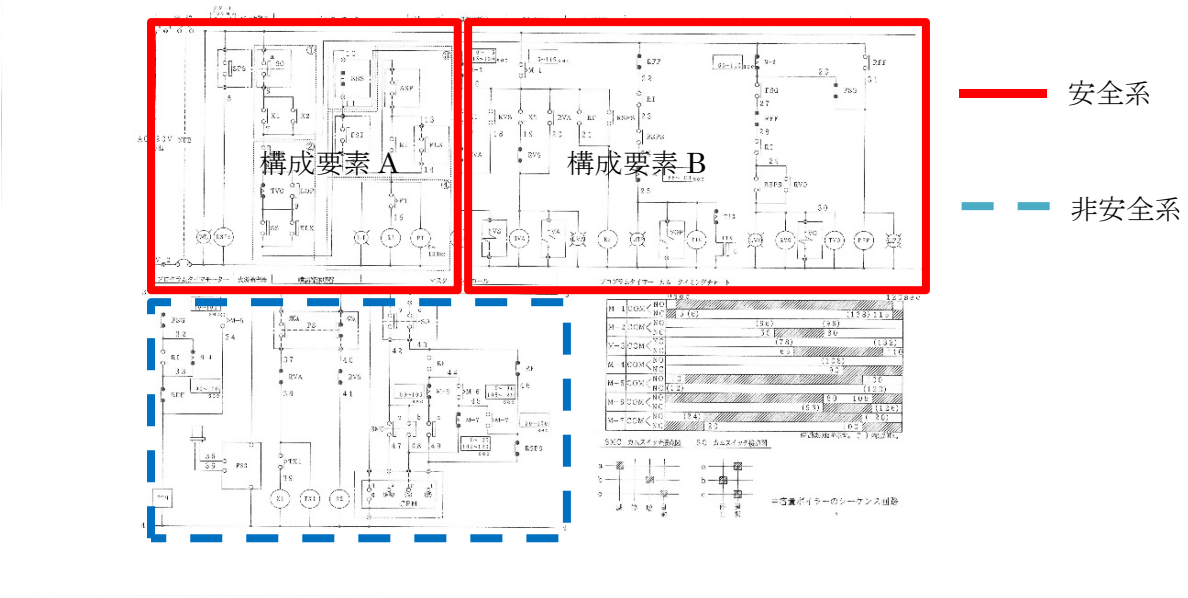


図３　安全関連システムの回路図の記載事例（回路は任意）

（イ） 機能ブロック図

製品の構成要素の機能ブロック図を回路図の情報をもとに作成する。
FMEDA の評価は機能ブロック毎に実施する場合がある。

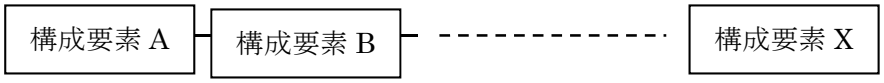


図４　製品の機能ブロック図の例

（ウ） 故障率

IEC 61800-5-2 AnnexC より抜粋した故障率のハンドブックを以下に示す。

・ **IEC/TR 62380, Reliability data handbook – Universal model for reliability prediction of electronics components, PCBs and equipment**, identical to RDF 2000/Reliability Data Handbook, UTE C 80-810, Union Technique de l'Electricité et de la Communication (www.ute-fr.com).
・ **Siemens Standard SN 29500, Failure rates of components**, (parts 1 to 14); can be obtained from: Siemens AG, CT SR SI, Otto-Hahn-Ring 6, D-81739, Munich.
・ **Reliability Prediction of Electronic Equipment, MIL-HDBK-217E**, Department of Defense, Washington DC, 1982.
・ **Reliability Prediction Procedure for Electronic Equipment**, Telcordia SR-332, Issue 01, May 2001 (telecom-info.telcordia.com), (Bellcore TR-332, Issue 06).
・ **EPRD – Electronic Parts Reliability Data (RAC-STD-6100)**, Reliability Analysis Center,201 Mill Street, Rome, NY 13440 (rac.alionscience.com).
・ **NPRD-95 – Non-electronic Parts Reliability Data (RAC-STD-6200)**, Reliability Analysis Center, 201 Mill Street, Rome, NY 13440 (rac.alionscience.com).
・**British Handbook for Reliability Data for Components used in Telecommunication Systems**, British Telecom (HRD5, last issue).

・ **Chinese Military Standard GJB/z 299B**.
・ **AT&T reliability manual** – Klinger, David J., Yoshinao Nakada, and Maria A. Menendez, Editors,l, AT&T Reliability Manual, Van Nostrand Reinhold, 1990, ISBN:0442318480.
・ **FIDES** – (FIDES is a new (January 2004) reliability data handbook developed by a consortium of French industry under the supervision of the French DoD DGA). FIDES is available on request at fides@innovation.net.
・ **IEEE Gold book** – The IEEE Gold book IEEE recommended practice for the design of reliable, industrial and commercial power systems provides data concerning equipment reliability used in industrial and commercial power distribution systems. IEEE Customer Service, 445 Hoes Lane, PO Box 1331, Piscataway, NJ, 08855-1331, U.S.A., Phone: +1 800 678 IEEE (in the US and Canada) +1 732 981 0060 (outside of the US and Canada),FAX: +1 732 981 9667 e-mail: customer.service@ieee.org.
・ **IRPH ITALTEL Reliability Prediction Handbook** – is the Italian telecommunication companies version of CNET RDF. The standards are based on the same data sets with only some of the procedures and factors changed. The Italtel IRPH handbook is available on request from: Dr. G Turconi, Direzione Qualita, Italtel Sit, CC1/2 Cascina Castelletto,20019 Settimo Milanese Mi., Italy.
・ **PRISM** (RAC / EPRD) – The PRISM software is available from the address below, or is incorporated within several commercially available reliability software packages: The Reliability Analysis Center, 201 Mill Street, Rome, NY 13440-6916, U.S.A.

以上は FMEDA や信頼性評価のベースになりうるが、故障率のハンドブックに記載された数学的モデルによる故障率の評価は、一般には難しいものもある。一方、EN 13611 では実用性のある故障率データが記載されているので、付録 1 に、EN 13611 の故障率を示した。

・ EN 13611:2007 + A2:2011 Safety and control devices for gas burners and gas burning applications – General requirements

故障率のデータブックは評価方法がそれぞれ異なっている。従って、恣意的に低い故障率となるようにデータを選択することは好ましくない。なお、上記のデータブックの一部は改訂されているので最新版を入手すること。また、上記のデータブックは大半が有償であるが、国内では、下記においていくつかのデータブックの調査が行われているので参考とされると良い。

機能安全規格の解説と SIL(ASIL)評価のための電子部品故障率予測ガイドライン
平成 25 年度　電子部品信頼性調査研究委員会研究成果報告書
平成 26 年 3 月　一般財団法人　日本電子部品信頼性センター

現状では、部品の故障率データは、ベンダーから入手することが最も確実である。不足部品については、EN 13611 や上述のハンドブックなどから求める必要がある。

（エ）故障モード

コンポーネントの故障モードの出典には以下がある。

- **IEC/TR 62380, Reliability data handbook – Universal model for reliability prediction of electronics components, PCBs and equipment**, identical to RDF 2000/Reliability Data Handbook, UTE C 80-810, Union Technique de l'Electricité et de la Communication (www.ute-fr.com).

・IEC 62061 Edition 1.0 2005-01 Safety of machinery - Functional safety of safety-related electrical, electronic and programmable electronic control systems

・Failure Mode / Mechanism Distributions - FMD-2016, Reliability Information Analysis Center

・EN 13611:2007 + A2:2011 Safety and control devices for gas burners and gas burning applications - General requirements

FMEDA では、部品の故障モード毎に、故障の結果、「安全側」になるか「危険側」になるかについて判定を行う。タイプ B 製品や ASIC などの複雑な部品のような故障モードの詳細分析が不可能な場合には、一般に安全側故障:危険側故障=50%:50%の仮定が受け入れられている。

また、故障しても安全機能に影響しない「No Effect Failure」と安全機能に含まれない「No Part Failure」がある。

FMD の故障モード数はかなり多い。IEC/TR62380、IEC 62061 及び EN 13611 は、比較的少なく扱いやすい。

付録 1 には EN 13611 の単純な故障モードが故障率とともに示されている。

（オ）診断率

自動的な診断テストで検出される故障モードを決定することが必要であり、一般に単純なコンポーネント（抵抗、コンデンサ、トランジスタ）の開回路、短絡故障のような故障であれば100%検出可能であると考えられている。

また、自己診断機能があるような部品の診断率は、IEC 61508 第2部の付属書A 表A.1から表A.16に示されているが、使用する診断技術によって診断率は低(60%)、中(90%)及び高(99%)に制約される。すなわち、制約された診断率までは使用することが可能である。付録2にEN 13611の診断率の表を示すが、そのベースはIEC 61508 第2部の付属書Aである。設計者はこれらの情報をもとにして部品単位の診断率を決定する必要がある。

（カ）フォールトトレランス

安全関連システムが危険側に機能喪失を引き起こすことのないランダムハードウェア故障から生じるサブシステムの最大のフォールト数として定義される。表１には、様々な構成のハードウェアフォールトトレランスを示す。

表１　ハードウェアフォールトトレランス

構成	ハードウェアフォールトトレランス
1oo1	0
1oo2	1
1oo3	2
2oo2	0
1oo2D	1
2oo3	1

1oo1のサブシステムであれば、1故障で機能を喪失するためハードウェアフォールトトレランスは0、1oo2であれば1故障しても機能が達成できるので、ハードウェアフォールトトレランスは１になる。ただし、同じ2重系であっても、2oo2 は危険側故障に対するハードウェアフォールトトレランスは 0である。

（キ）製品のタイプ

製品の挙動の明確さ等によって製品はタイプAとタイプBに分けられる。安全機能を達成するのに必要なコンポーネントが以下を全て満たせば、要素はタイプAとみなされる。

a）すべての構成するコンポーネントの故障モードが、よく定義される。
b）フォールト条件下の要素の挙動が完全に決定できる。
c）検知可能及び検知不可危険側故障に対して主張された故障率に合うことを示す十分に信頼できる故障データがある。

一方、以下のうち一つでもあてはまれば、要素はタイプBとみなされる。

a）少なくとも、1つのコンポーネントの故障モードがよく定義されない。
b）フォールト条件下の要素の挙動が完全には決定できない。

c）検知不可及び検知不可危険側故障に対する故障率の主張を支援する信頼できる故障データが不十分である。

初めて、認証審査を行う場合には、タイプBで申請する例が一般的であり、後にタイプAに変更する例もある。

ウ　運転情報

（ア） 使用環境（温度、振動等）

FMEDAを評価する場合に、使用温度に範囲がある場合には、温度に感受性のある部品の故障率が変化することがある。また、振動やダストなどの安全関連システムの設置環境が劣悪である場合にも故障率が変化する可能性がある。使用する故障率データブックには、このような環境の補正ファクターが定義されているものがあるので、該当するような環境に接地する場合には補正が必要である。

可能な限り、温和な環境に設置して故障率が増加することがないようにする方が望ましい。

（２）FMEDA

エ　計算

（ア）FMEDA の評価

（１）製品の情報からの情報を用いて表２の FMEDA シートを使用して FMEDA を実施する。FMEDA では安全関連システムを構成する製品の安全機能に関わる部品について、部品の故障率λ（FIT）をもとにして、(2)～(5)によって、次の４種類の故障率を計算する。

$\lambda = \lambda_S + \lambda_D$ (1)

$\lambda_{SD} = \lambda_S \times DC$ (2)

$\lambda_{SU} = \lambda_S \times (1-DC)$ (3)

$\lambda_{DD} = \lambda_D \times DC$ (4)

$\lambda_{DU} = \lambda_D \times (1-DC)$ (5)

ここで；

λ ；全故障率（FIT）

λ_S；安全側故障率（FIT）

λ_D；危険側故障率（FIT）

DC；自己診断率（-）

λ_{SD}；検知可能安全側故障率(FIT)

λ_{SU}；検知不可安全側故障率(FIT)

λ_{DD}；検知可能危険側故障率(FIT)

λ_{DU}；検知不可危険側故障率(FIT)

IEC 61508 ではλ_{SD}、λ_{SU}、λ_{DD}、λ_{DU}の他に下記の故障率が定義されている。

λno　effect failure；安全機能に含まれるが、機能の遂行に影響しない部品の故障率（FIT）

λno part failure　；安全機能に含まれない部品の故障率（FIT）

λno　effect failure とλno part failure は（イ）に示す安全側故障割合（SFF）の計算には含まれない。

（イ） 安全側故障割合（SFF）

回路全体でλ_{SD}、λ_{SU}、λ_{DD}、λ_{DU}の集計を行い、(6)、(7)式によって、回路全体の安全側故障割合(SFF;Safe Failure Fraction)診断率(DC;Diagnostic Coverage)を計算する。

$$SFF = \frac{\sum \lambda_{SD} + \sum \lambda_{SU} + \sum \lambda_{DD}}{\sum \lambda_S + \sum \lambda_D} \quad (6)$$

Σは、サブシステムまたはサブシステムの構成要素の部品の故障モードのすべてに渡って集計することを意味する。

SFF は表 5 又は表 6 によって製品のアーキテクチャ制約を評価するために使用される。

（ウ） 診断率（DC）

回路全体の診断率（DC）を、(7)式によって計算する。

$$DC = \frac{\sum \lambda_{DD}}{\sum \lambda_{D}} \qquad (7)$$

DC は IEC 61508 第 6 部の計算式によって PFDavg を計算する場合に入力値として使用される。

以上の情報を用いて実施する FMEDA の評価に用いる表の例を表 2 に示す。

表 2　FMEDA 評価シートの例

番号	部品名称	全故障率 (FIT)	故障モード	分配率 (%)	故障率 (FIT)	安全側/危険側	診断率 (%)	λ_{SD} (FIT)	λ_{SU} (FIT)	λ_{DD} (FIT)	λ_{DU} (FIT)	$\lambda_{\text{No Effect Failure}}$ (FIT)	$\lambda_{\text{No Part Failure}}$ (FIT)
1	sample-1	120.00	接続の開回路	25	30.00	危険側故障(D)	60.00	0.00	0.00	18.00	12.00	0.00	0.00
			2 つの接続間短絡	25	30.00	安全側故障(S)	60.00	18.00	12.00	0.00	0.00	0.00	0.00
			すべての接続間短絡	25	30.00	50%安全側、50%危険側	60.00	9.00	6.00	9.00	6.00	0.00	0.00
			特性変化	25	30.00	対象外(no effect)	60.00	0.00	0.00	0.00	0.00	30.00	0.00
6	sample-2	15.00	接続の開回路	25	3.75	危険側故障(D)	60.00	0.00	0.00	2.25	1.50	0.00	0.00
			2 つの接続間短絡	25	3.75	安全側故障(S)	60.00	2.25	1.50	0.00	0.00	0.00	0.00
			すべての接続間短絡	25	3.75	安全側故障(S)	60.00	2.25	1.50	0.00	0.00	0.00	0.00
			特性変化	25	3.75	50%安全側、50%危険側	60.00	1.13	0.75	1.13	0.75	0.00	0.00
2	sample-3	3.00	接続の開回路	25	0.75	危険側故障(D)	90.00	0.00	0.00	0.68	0.08	0.00	0.00
			2 つの接続間短絡	25	0.75	安全側故障(S)	90.00	0.68	0.08	0.00	0.00	0.00	0.00
			すべての接続間短絡	25	0.75	安全側故障(S)	60.00	0.45	0.30	0.00	0.00	0.00	0.00
			特性変化	25	0.75	50%安全側、50%危険側	60.00	0.23	0.15	0.23	0.15	0.00	0.00
①	②	③	④	⑤	⑥	⑦	⑧	⑨	⑩	⑪	⑫	⑬	⑭

① 番号；通し番号
② 部品名称
③ 全故障率（FIT）
④ 故障モード
⑤ 分配率（%）
⑥ 故障率（FIT）；故障モードに配分された故障率（全故障率③×分配率⑥/100）
⑦ 安全側/危険側
⑧ 診断率（%）；診断で検知できる故障の割合
⑨ λ_{SD}(FIT) 検知可能安全側故障率
⑩ λ_{SU}(FIT) 検知不可安全側故障率
⑪ λ_{DD}(FIT) 検知可能危険側故障率
⑫ λ_{DU}(FIT) 検知不可危険側故障率

⑬　$\lambda_{\text{No Effect Failure}}$(FIT) 安全機能に影響しない部品の故障率
⑭　$\lambda_{\text{No Part Failure}}$(FIT) 安全機能に含まれない部品の故障率

（エ） PFDavg の計算

PFDavg を、IEC 61508 第 6 部の計算式によって計算し、IEC 61508 第 1 部の安全度水準の目標失敗尺度と比較して安全度水準を求める。低頻度モードの場合を表 3 に、高頻度・連続モードの場合を表 4 に示す。本ガイドラインでは PFDavg の事例を示す。

表 3　安全度水準－低頻度モード運用の安全機能の作動要求あたりの目標失敗尺度

安全度水準（SIL）	安全機能の作動要求あたりの平均危険側失敗確率(PFDavg)
4	$\geqq 10^{-5} \sim < 10^{-4}$
3	$\geqq 10^{-4} \sim < 10^{-3}$
2	$\geqq 10^{-3} \sim < 10^{-2}$
1	$\geqq 10^{-2} \sim < 10^{-1}$

表 4　安全度水準－高頻度・連続モード運用の安全機能の作動要求あたりの目標失敗尺度

安全度水準（SIL）	安全機能の平均危険側失敗頻度(PFH)
4	$\geqq 10^{-9} \sim < 10^{-8}$
3	$\geqq 10^{-8} \sim < 10^{-7}$
2	$\geqq 10^{-7} \sim < 10^{-6}$
1	$\geqq 10^{-6} \sim < 10^{-5}$

IEC 61508 第 6 部の式は、アーキテクチャ構成が合致している場合にだけ使用できる。
非対称の 2 重系や複雑な構成の場合には、マルコフモデルなどで計算しなければならない。特に、故障時の回路の挙動などを分析するためには、マルコフモデルやフォールトツリーによる挙動の分析が重要である。

（３）アーキテクチャ制約

サブシステムのとり得る最大の SIL は、安全側故障割合（SFF)、製品の新規性や複雑度で決定される製品タイプ A/B 及び冗長度で決定されるハードウェアフォールトトレランスの 3 つの因子によって決定される。

IEC 61508 第 2 部 から表 5（製品タイプ A の場合）又は表 6（製品タイプ B の場合）によって、サブシステムのアーキテクチャ制約について検討する。

表 5　タイプ A 安全関連要素またはサブシステムによって実行された安全機能の許容される最大の安全度水準

安全側故障割合	ハードウェアフォールトトレランス		
	0	1	2
<60%	SIL1	SIL2	SIL3
60% ≦ 90%	SIL2	SIL3	SIL4
90% ≦ 99%	SIL3	SIL4	SIL4
≧99%	SIL3	SIL4	SIL4

表 6　タイプ B 安全関連要素またはサブシステムによって実行された安全機能の許容される最大の安全度水準

安全側故障割合	ハードウェアフォールトトレランス		
	0	1	2
<60%	不可	SIL1	SIL2
60% ≦ 90%	SIL1	SIL2	SIL3
90% ≦ 99%	SIL2	SIL3	SIL4
≧99%	SIL3	SIL4	SIL4

例えば、製品タイプ、安全側故障割合（SFF）ハードウェアフォールトトレランスの組み合わせによって、表 5、表 6 に示される SIL までは主張できる（認められる）ことを意味している。安全側故障をする部品を含めば含むほど、SFF が大きくなるので SIL が増加するが、恣意的にこのような設計を行うことは認められるべきことではない。

（４）フォールト注入試験

実際に、短絡や断線を模擬したフォールトを注入して設計で想定している動作が得られるかどうかを確認する。全数の試験が困難な場合には、選定基準を作成して試験を実施する部品を選定する。試験は FMEDA の結果をもとにして高い故障率を有し、診断で検知できると判断している部品を主に選定する。

（５）安全マニュアル

サブシステムやサブシステムの構成要素のサプライヤーは、システム統合をする組織が必要な情報を IEC 61508 第 2 部付属書 D に従って安全マニュアルを作成して提供する。

２．２システムの評価

図２に従ってシステムの評価を行うための情報の入手や計算方法について以下に解説する。

(6) システムの情報

ア　安全要求仕様

（ア）安全機能と要求安全度

製品の評価と同じように安全要求仕様の情報を参照する。

イ　運用情報

（ア） 運用モード

作動要求頻度が１回/年を超える場合は、高頻度・連続作動要求モードの時間あたりの危険側故障確率 PFH を評価する。下回る場合は、低頻度作動要求モードの作動要求あたりの危険側平均故障確率 PFDavg を評価する。本マニュアルでは、低頻度作動要求モードの場合を想定している。

（イ） プルーフテスト間隔

安全関連系の故障状態を見つけるためにシステムを停止して実施される周期点検のテストのことをいい、故障を検知した場合には、システムを‘新品’又は実際上これに近い状態に修復する。プルーフテスト間隔は PFDavg の計算に使用され、短ければ短い程、SIL は増大する。

> オンラインで自動診断する場合に検知できない故障が、プルーフテストで検知されることが望ましい。プルーフテストで、故障が完全に検知できるかどうかによっては、PFDavg の値が変わる。プルーフテストの設備についても適宜、仕様書等において言及する。

（ウ） 平均修理時間（MRT）

IEC 61508 第 4 部 3.6.21、3.6.22 によれば、MRT は故障を検知した後に、運転に戻るまでの時間であり、平均修復時間 MTTR から故障を検知する時間を差し引いた時間として定義される。

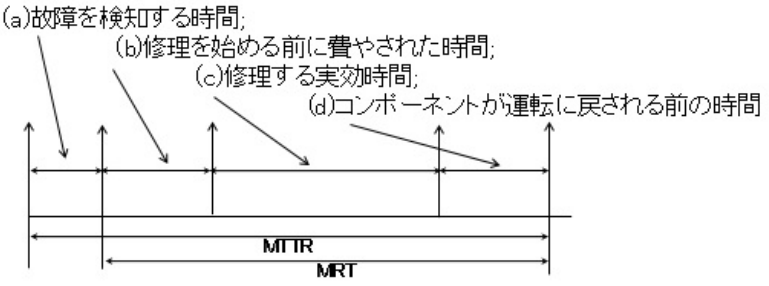


図５　MRT と MTTR の関係

PFDavg の計算では、MRT と MTTR が使用される。オンラインの自動診断で検知された故障を修理、又は交換するために要する時間が図 5 の MRT 以内であることの保証が必要である。

（７）PFDavg の計算

ウ　　評価

（ア）　信頼性ブロック図

図６のシステムの機能ブロック図をもとにして、図７の信頼性ブロック図を作成する。

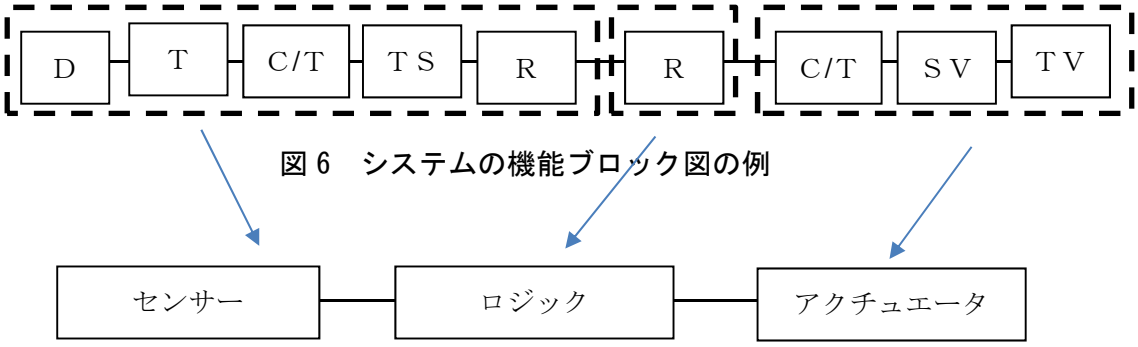


図６　システムの機能ブロック図の例

図７　システムの信頼性ブロック図の例

（イ）共通原因故障割合

システムやサブシステムが多重になっている場合には、共通原因故障についての評価が必要になる。ただし、多様な技術を使用した多重系の場合には、共通原因による故障は考慮しなくても良い場合がある。
共通原因故障割合は、一般にβファクターと呼ばれる。
IEC 61508 第６部付属書Ｄの評価方法を参照してβファクターを求める。
評価方法は 3.2.1 で解説する。また、付録３には IEC 61508 の評価モデルよりも簡単な EN 13611 の評価モデルを示したので参照されたい。

（ウ）PFDavg の計算

センサーが１重系の場合と２重系の場合の PFDavg の計算例を以下に示す。

［１重系の例］
機能ブロック図に示した構成要素の危険側故障率を表７に示す。

表７　構成要素の危険側故障率

記号	構成要素	λ_D危険側故障率（FIT）
D	検知器	10,000
T	トランズミッタ	5,000
C／T	ケーブル/端子	0
T S	トリップアンプ・スイッチ	10,000
R	リレー	200
S V	ソレノイドバルブ	2,000
T V	トリップバルブ	10,000

注　例示のために故障率は任意の値としている。

表 5 より；

センサーの危険側故障率（FIT）

λ_{DS}＝10000＋5000＋0＋10000＋200＝25200

ロジックの危険側故障率（FIT）

λ_{DL}＝200

アクチュエータの危険側故障率（FIT）

λ_{DA}＝200＋2000＋10000＝12200

となる。

T1：プルーフテスト間隔(点検周期)（時間）
MRT：平均修理時間（時間）
MTTR：平均修復時間（時間）
DC：診断率（-）
とすると；

IEC 61508 第 6 部付属書 B3.2.2.1 より、

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR \quad (8)$$

$$\lambda_{DU} = \lambda_D(1 - DC) \quad (9)$$

$$\lambda_{DD} = \lambda_D DC \quad (10)$$

$$PFD_G = (\lambda_{DU} + \lambda_{DD})t_{CE} \quad (11)$$

t_{CE};チャンネル等価平均ダウンタイム（時間）
λ_D；危険側故障率（－/時間）
λ_{DD}；検知可能危険側故障率（－/時間）
λ_{DU}；検知不可危険側故障率（－/時間）
PFD_G；作動要求あたりの危険側失敗確率（－）

注 1 IEC 61508 第 6 部付属書 B においては、作動要求あたりの危険側失敗確率の評価式に PFD_G を使用しているところがあるが、PFDavg と同じ意味である。

注 2　(8)式で、MTTR と MRT の差が PFDavg 計算に影響する場合には、異なる値にする必要がある。ここでは、簡単にするため、計算例では MTTR と MRT はともに８時間とした。

(センサー)
DC =0.85（FMEDA で決定される）
λ_D = 25200 × 10^{-9} (-/時間) ；25200 FIT（FMEDA で決定される）
T_1 = 1（年）（8760 時間）
MRT = 8　（時間）
MTTR = 8　（時間）

λ_{DD} = 25200 × 10^{-9} × 0.85 = 2.142 × 10^{-5}(-/時間) ; 21420 FIT
λ_{DU} = 25200 × 10^{-9} × (1 - 0.85) = 3.780 × 10^{-6}(-/時間) ;3780 FIT
t_{CE} = (3780/25200) × (8760/2 + 8) + (21420/25200)× 8 = 665 (時間)
PFD_G = (2.142 × 10^{-5} + 3.780 × 10^{-6}) × 665 = 1.676 × 10^{-2} (-)

(ロジック)
DC =0.6 (FMEDA で決定される)
λ_D = 200 × 10^{-9} (-/時間) ; 200 FIT (FMEDA で決定される)
T_1 = 1 (年) (8760 時間)
MRT = 8 (時間)
MTTR = 8 (時間)

λ_{DD} = 200 × 10^{-9} × 0.85 = 1.20 × 10^{-7}(-/時間) ; 120 FIT
λ_{DU} = 200 × 10^{-9} × (1 - 0.6) = 8.0 × 10^{-8}(-/時間) ;80 FIT
t_{CE} = (80/200) × (8760/2 + 8) + (120/200)× 8 = 1760 (時間)
PFD_G = (1.20 × 10^{-7} + 8.0 × 10^{-8}) × 1760 = 3.520 × 10^{-4} (-)

(アクチュエータ)
DC =0.9 (FMEDA で決定される)
λ_D = 12200 × 10^{-9} (-/時間) ; 12200 FIT (FMEDA で決定される)
T_1 = 0.5 (年) (4380 時間)
MRT = 8 (時間)
MTTR = 8 (時間)

λ_{DD} = 12200 × 10^{-9} × 0.9 = 1.098 × 10^{-5}(-/時間) ; 10980 FIT
λ_{DU} = 12200 × 10^{-9} × (1 - 0.9) = 1.220 × 10^{-6}(-/時間) ;1220 FIT
t_{CE} = (1220/12200) × (4380/2 + 8) + (10980/12200)× 8 = 227 (時間)
PFD_G = (1.098 × 10^{-5} + 1.220 × 10^{-6}) × 227 = 2.769 × 10^{-3} (-)

各サブシステムの計算条件 (想定値) と計算結果を表 8 にまとめた。

表 8　サブシステムの計算条件と結果（センサーが 1 重系の例）

項目	センサー	ロジック	アクチュエータ
危険側故障率 λ_D（FIT） 注1	25200	200	12200
DC	0.85	0.6	0.9
検知不可危険側故障率 λ_{DU}（FIT）	3780	80	1220
検知可能危険側故障率 λ_{DD}（FIT）	21420	120	10980
プルーフテスト間隔 T_1（年） 注2	1	1	0.5
平均修理時間MRT(時間)	8	8	8
平均修復時間MTTR(時間)	8	8	8
tCE （時間）	665.0	1760.0	227.0
PFDG	1.676E−02	3.520E−04	2.769E−03
SIL	1	3	2

注1　計算では 1 時間あたりの故障数に換算する（$\times 10^{-9}$）。
注2　計算では時間に換算する（×8760）。

センサー、ロジック、アクチュエータが相互に独立している場合には、安全関連システムの PFDavg は、それぞれのサブシステムの PFDavg を足し算して求めることができる。

（ランダムハードウェア故障確率）

PFDavg = 1.676E-2 + 3.520E-4 + 2.769E-3　=　1.988E-2

この PFDavg は、表 3 より、SIL1 となる。

注 1　センサー、ロジック、アクチュエータが独立していない場合には、単純な足し算で求めることはできない。マルコフモデルのような信頼性モデルを使用して計算することが必要になる。

［2 重系の例］

（信頼性ブロック図）
センサーが 2 重化されている場合の信頼性ブロック図を図 8 に示す。

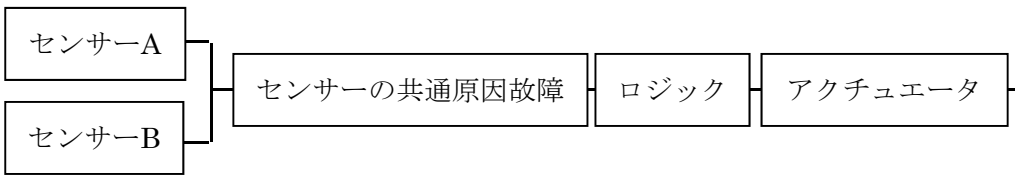


図 8　2 重化システムの信頼性ブロック図の例

センサーA、B の危険側故障率（FIT）を

λ_{DSA}＝25200

λ_{DSB}＝25200

とし、ロジックとアクチュエータは 1 重系の場合と同じ危険側故障率とする。

センサーの部分の PFD_G は IEC 61508 第 6 部付属書 B3.2.2.1 より、

$$t_{GE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{3} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR \quad (12)$$

$$PFD_G = 2((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU})^2 t_{CE} t_{GE} + \beta_D \lambda_{DD} MTTR + \beta\lambda_{DU}\left(\frac{T_1}{2} + MRT\right) \quad (13)$$

t_{GE}；チャンネル等価平均ダウンタイム(時間)
β ；診断で検知されない共通原因故障の割合(%)
β_D；診断で検知される共通原因故障の割合(%)

(センサー)
DC =0.85（FMEDA で決定される）
λ_D = 25200 × 10^{-9} (-/時間) ； 25200 FIT（FMEDA で決定される）
T_1 = 1（年）（8760 時間）
MRT = 8 （時間）
MTTR = 8 （時間）
β = 2（%）;3.2.1 の導出方法を参照。
β_D = 1（%）;3.2.1 の導出方法を参照。

λ_{DD} = 25200 × 10^{-9} × 0.85 = 2.142 × 10^{-5}(-/時間) ; 21420 FIT
λ_{DU} = 25200 × 10^{-9} ×（1 - 0.85 ）= 3.780 × 10^{-6}(-/時間) ;3780 FIT
t_{CE} =（3780/25200）×（8760/2 + 8 ）+（21420/25200)× 8 = 665（時間 ）
t_{GE} =（3780/25200）×（8760/3 + 8 ）+（21420/25200)× 8 = 446（時間 ）

PFD_G = 2((1-0.01) × 2.142 × 10^{-5} + (1 - 0.02) × 3.780 × 10^{-6})^2 × 665 × 446 + 0.01 × 2.142 × 10^{-5} × 8 + 0.01 × 3.780 × 10^{-6}× 8 + 0.02 × 2.142 × 10^{-5} ×（8760/2 + 8 ）= 7.015 × 10^{-4} (-)

ロジックとアクチュエータは 1 重系の例と同じである。各サブシステムの計算条件と計算結果を表 9 にまとめた。

表 9　サブシステムの計算条件と結果（センサーが 2 重系の例）

項目	センサー	ロジック	アクチュエータ
危険側故障率 λ_D（FIT） 注1	25200	200	12200
DC	0.85	0.6	0.9
検知不可危険側故障率 λ_{DU}（FIT） 注1	3780	80	1220
検知可能危険側故障率 λ_{DD}（FIT） 注1	21420	120	10980
プルーフテスト間隔 T_1（年） 注2	1	1	0.5
平均修理時間MRT (時間)	8	8	8
平均修復時間MTTR (時間)	8	8	8
tCE （時間）	665.0	1760.0	227.0
tGE （時間）	446.0	−	−
β D(%) 注3	1.0	−	−
β (%) 注3	2.0	−	−
PFDG	7.015E−04	3.520E−04	2.769E−03
SIL	3	3	2

注1　計算では 1 時間あたりの故障数に換算する（$\times 10^{-9}$）。
注2　計算では時間に換算する（×8760）。
注3　計算では少数に換算する（×0.01）。

1 重系の場合と同様に、センサー、ロジック、アクチュエータが相互に独立している場合を想定して、それぞれのサブシステムの PFDavg を足し算して安全関連システムの PFDavg を求める。

（ランダムハードウェア故障確率）
PFDavg = 7.015E-4 + 3.520E-4 + 2.769E-3　=　3.823E-3

この PFDavg は、表 3 より、SIL2 となる。

（8）アーキテクチャ制約

システムのアーキテクチャ制約の要求により、最小の SIL を有するサブシステムの SIL によってシステム全体の SIL が制約される

（1 重系の場合）
ランダムハードウェア故障確率の計算からはシステム全体の SIL は 1 であり、かつ、表 8 から、センサーの SIL1 によって制約されて全体システムの SIL は 1 になる。

従って、ランダムハードウェア故障確率計算とアーキテクチャ制約の両者ともに SIL 1 になり、システムは SIL1 となる。

（2 重系の場合）
ランダムハードウェア故障確率の計算からはシステム全体の SIL は 2 であり、かつ、表 9 から、アクチュエータの SIL2 によって制約されて全体システムの SIL は 2 になる。

従って、ランダムハードウェア故障確率計算とアーキテクチャ制約の両者ともに SIL2 になり、システムは SIL2 となる。

３　ボイラーのＳＩＬの評価例

ボイラーでは、1oo1 と 1oo2 の安全関連システムが多く使用されている。ここでは、ボイラーの安全関連システムの事例をもとにして SIL の評価をより具体的に解説する。3.1 に製品の PFDavg、3.2 にシステムの PFDavg の計算の例を示した。なお、使用した故障率のデータなどは、全て仮想的な値である。実際にボイラーの安全関連システムを評価する場合には、本マニュアルの評価手順を参考にして使用条件および使用データを十分に吟味して決定することが必要である。なお、付録１～３に EN 13611 の故障率、故障モード及び自己診断率の表を添付した。

３．１　製品の PFDavg

図 9 に、EN 13611 の故障率、故障モード及び自己診断率と FMEDA 表との関係を示す。図 9 に従って、表 2 の FMEDA 用のシートに必要事項を入力していく。

（１）部品の故障率、故障モード

設計者は、安全関連システムの製品に使用した全ての部品について入力する。

（２）自己診断率

個別の部品について、自己診断率を入力する。診断が不可能な場合には、ゼロを入力する。

（３）集計計算

部品毎にλSD、λSU、λDD、λDU を計算して集計する。

（４）SFF の計算

(6)式によって SFF を計算する。

例えば；

$\Sigma\lambda_{DD}$ = 450、$\Sigma\lambda_{DU}$ = 200、$\Sigma\lambda_{SD}$ = 600、$\Sigma\lambda_{SU}$ = 90 の場合には；

$\Sigma\lambda_{D}$ = 650

$\Sigma\lambda_{S}$ = 690

$$SFF = \frac{600 + 90 + 450}{690 + 650} = 0.850$$

となり、安全側故障割合は 85.0％となる。

（５）DC の計算

(7)式によって DC を計算する。

上記の数値を使用すると；

$$DC = \frac{450}{650} = 0.692$$

となり、診断率は 69.2%となる。

（６）製品タイプ

本事例では新製品であることを想定してタイプ B とする。

（７）アーキテクチャ制約の評価

タイプ B のアーキテクチャ制約の表 6 を用いて、主張できる最大の SIL を評価する。

表 6　タイプ B 安全関連要素またはサブシステムによって実行された安全機能の許容される最大の安全度水準

安全側故障割合	ハードウェアフォールトトレランス		
	0	1	2
<60%	不可	SIL1	SIL2
60% ≦ 90%	~~SIL1~~	SIL2	SIL3
90% ≦ 99%	SIL2	SIL3	SIL4
≧99%	SIL3	SIL4	SIL4

例えば、製品タイプが B、安全側故障割合が 85%、ハードウェアフォールトトレランスが 0(1 重系)の場合とすると、SIL1 となる。

番号	部品名称	全故障率(FIT)	故障モード	分配率(%)	故障率(FIT)	安全側/危険側	診断率(%)	λ_{SD}(FIT)	λ_{SU}(FIT)	λ_{DD}(FIT)	λ_{DU}(FIT)	$\lambda_{No\ Effect\ Failure}$(FIT)	$\lambda_{No\ Part\ Failure}$(FIT)
1	抵抗 001	8.0	ショート	50	4.00	危険側故障(D)	100.00	0.00	0.00	4.00	0.00	0.00	0.00
			オープン	50	4.00	安全側故障(S)	0.0	0.00	4.00	0.00	0.00	0.00	0.00

Component type	failure modes							failure rates	
	short	open	Drift 1/2x	Drift 2x	others	no. of pins	no. of faults	component failure rate λ [fit] a	failure rate per fault [fit]
Column	1	2	2a	2b	2c	3	4	5	6
Resistors									
Carbon film		1				2	1	1,6	1,6
Metal film		1				2	1	0,3	0,3
Metal oxide		1				2	1	8,0	8,0
Wire wound	1	1				2	2	8,0	4,0
Networks per resistor element	1	1				2	2	0,2	0,1
Variable resistors									
Wire wound (single layer)		1				3	3	48,0	16,0
All other	1	1				3	6	48,0	8,0
Varistors	1	1				2	2	1,0	0,5
PTC thermistors	1	1	1	1		2	4	5,0	1,25
NTC thermistors	1	1	1	1		2	4	3,0	0,75

設計者が、故障の結果、危険側になるか安全側になるかを判断する。

設計者が、故障を検知できるかどうかを決定する。自動診断が適用される場合には付録 2 を参照して診断率を決定する。

図９　FMEDA の入力事項（EN 13611 を使用した例）

（８）サブシステムの PFDavg の計算

IEC 61508 の第 6 部には、運転中の自己診断によって故障を検知した場合に修理・交換を行う場合の PFDavg の式が掲載されているが、自己診断機能がなくて数日の短い点検周期で点検するような場合や、故障を検知すると直ちに安全側に停止するような場合と対応していない。従って、ボイラーでは、このような場合があり得ることを考慮して、多く使用されている 1oo1 と 1oo2 の安全関連システムに適用しうる PFDavg の計算式を以下に示す。

ア 1oo1

IEC 61508 第 6 部付属書 B3.2.2.1 から、1oo1 の場合には運転中に自己診断が可能であり、かつ、故障を検知した場合に運転中に修理・交換する場合には、2 章の（8）～（11）式が適用される。

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR \quad (8)$$

$$\lambda_{DU} = \lambda_D(1 - DC) \quad (9)$$

$$\lambda_{DD} = \lambda_D DC \quad (10)$$

$$PFD_G = (\lambda_{DU} + \lambda_{DD})t_{CE} \quad (11)$$

DC は(7)式によって計算された値を使用する。

一方、自己診断機能がない場合には、運転中に故障検出ができないので、全ての危険側故障率 λ_D が検知不可危険側故障率 λ_{DU} となるので、下記が適用される。

$$t_{CE} = \frac{T_1}{2} + MRT \quad (14)$$

$$\lambda_{DU} = \lambda_D \quad (15)$$

$$PFD_G = \lambda_D t_{CE} \quad (16)$$

また、自己診断機能があって、運転中に故障を検知した場合に安全側に停止する場合には、下記が適用される。

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MRT\right) \quad (17)$$

$$\lambda_{DU} = \lambda_D(1 - DC) \quad (18)$$

$$\lambda_{DD} = \lambda_D DC \quad (19)$$

$$PFD_G = \lambda_{DU} t_{CE} \quad (20)$$

ただし、本マニュアルではこの場合に該当する事例を取り上げていない。

イ 1oo2

1oo2 の場合には、運転中に自己診断が可能であり、かつ、故障を検知した場合に運転中に修理・交換する場合には、2 章の（12）～（13）式が適用される

$$t_{GE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{3} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR \quad (12)$$

$$PFD_G = 2((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU})^2 t_{CE} t_{GE} + \beta_D \lambda_{DD} MTTR + \beta\lambda_{DU}\left(\frac{T_1}{2} + MRT\right) \quad (13)$$

一方、自己診断機能がない場合には、下記が適用される。

$$t_{CE} = \frac{T_1}{2} + MRT \quad (14)$$

$$t_{GE} = \frac{T_1}{3} + MRT \quad (21)$$

$$PFD_G = 2((1-\beta)\lambda_D)^2 t_{CE} t_{GE} + \beta\lambda_D\left(\frac{T_1}{2} + MRT\right) \quad (22)$$

2 重系の場合に自己診断機能があって、運転中に故障を検知した場合に安全側に停止する場合は、本マニュアルでは取り上げない。

３．２　システムのＰＦＤavg

システムで 1oo2 などの多重系が使用される場合の PFDavg の計算をする場合には、共通原因故障割合の評価が必要である。3.2.1 では共通原因故障割合の評価例を示す。また、3.2.2～3.2.4 ではボイラーの低水位/燃焼系遮断の構成例をもとにして、安全機能の PFDavg の計算事例を示した。

３．２．１　共通原因故障割合の評価

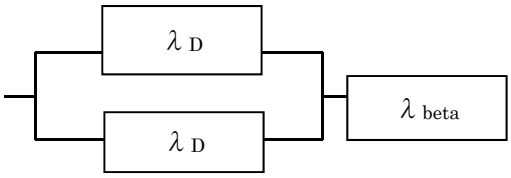
共通原因故障の原因には、以下のようなものがあるが、対策によって可能な限り共通原因故障の発生を抑制すべきである。

(a)　要求事項：不完全又は矛盾するもの
(b)　設計：共通の供給電源、ソフトウェア、EMC、ノイズ
(c)　製造：バッチに関連するコンポーネントの欠陥
(d)　保守・運用：要員の関与又は試験装置の問題
(e)　環境：温度サイクル、電気的な干渉等

後述の図１１～図１３のボイラーの低水位/燃焼系遮断の構成例（1）、（2）、（3）における遮断弁（MV1,MV2）　と構成例（2）のリレー（RY1、RY2）は 2 重化されているので、共通原因故障割合の評価が必要である。

共通原因故障を取り扱うβモデルが、IEC 61508 第 6 部付属書 D に示されている。この方法によって共通原因故障割合 β_D とβを求める方法と事例を以下に紹介する。

共通原因故障に関する信頼性ブロック図 10 を示す。



λ_D；単一のコンポーネントの危険側故障率
λ_{beta}；共通原因故障による危険側故障率
β ；単一のコンポーネントの故障率に対する共通原因故障の割合

図 10　共通原因故障の信頼性ブロック図

ここで、λ_{beta}は、λ_Dに共通原因故障割合βを乗じて求められる。

$$\lambda_{beta} = \beta \times \lambda_D \qquad (23)$$

さらに、危険側故障率λ_Dは診断で検知不可の危険側故障率λ_{DU}と、診断で検知可能な危険側故障率λ_{DD}に分けられる。

共通原因によって、同時に故障するわけではなく、一方が故障しても、他方が故障するまでに、故障が自己診断回路によって検知されると安全側にもたらすことが可能であるので、このモデルでは、それぞれの危険側故障率に対する共通原因故障割合を分けている。

共通原因故障による故障率；

$$\lambda_{beta} = \lambda_{DU}\beta + \lambda_{DD}\beta_D \qquad (24)$$

λ_{DU}；単一チャンネルの検知不可危険側故障率
β ：検知不可危険側故障の共通原因故障割合
λ_{DD}：単一チャンネルの検知可能危険側故障率
β_D：検知可能危険側故障の共通原因故障割合

βとβ_Dはスコア法によって求めることができる。
βを求めるときに使用するスコアは、次式による。

$$S = X + Y \qquad (25)$$

β_Dを求めるときに使用するスコアは、次式による。

$$S = X（Z + 1）+ Y \qquad (26)$$

X、Yの値は以下のスコア採点によって求められる。また、Zの値は診断機能の自己診断率と診断試験の間隔によって決定される。以下は評価の進め方を示す事例である。

遮断弁については、最終要素のスコアを用いて共通原因故障割合の評価を行うものとするが、診断機能がないので、(25) 式を用いてS値を求める。
構成例（２）のリレーについては、論理回路のスコアを用いて共通原因故障割合の評価を行う。

βとβ_Dを求めるIEC 61508のβモデルは、必ずしも設計を反映していない可能性もある。付録３に示すEN 13611のβモデルは、より簡単であるが、β_Dを求めるようにはなっていない。EN 13611や機械類について使用されているISO-13849-1やIEC 62061のスコア表もβ_Dを求めるようにはなっていないが、βとβ_Dを区別する必要がなければ使用について検討する余地がある。

〖ステップ１　質問への回答〗
次の分類に従って、論理回路とセンサー又は最終要素の該当部分のスコアを記録していく。

１．分離/隔離
２．多様性/冗長性
３．複雑さ/設計/用途/成熟度/経験
４．評価/データの解析とフィードバック
６．コンピテンシー/訓練/安全文化
７．環境のコントロール
８．環境試験

表１０の斜線部は該当していると判定した箇所である。

表１０ 共通原因故障割合の評価表

１．分離/隔離

項　　目	論理回路		センサー、最終要素	
	X_{LS}	Y_{LS}	X_{SF}	Y_{SF}
チャンネルの信号ケーブルは、全ての位置で分離して配線されているか？	~~1.5~~	~~1.5~~	~~1.0~~	~~2.0~~
論理回路のサブシステムは、分離したプリント基板上にあるか？	~~3.0~~	~~1.0~~		
論理回路のサブシステムは、分離したキャビネット内にあるか？	~~2.5~~	~~0.5~~		
センサー／最終要素に専用の制御用電子機器がある場合、各チャンネルの電子機器は内部にあって、分離したプリント基板上にあるか？			2.5	1.5
センサー／最終要素に専用の制御用電子機器がある場合、各チャンネルの電子機器は内部にあって、分離したキャビネット内にあるか			~~2.5~~	~~0.5~~

２．多様性/冗長性

項　　目	論理回路		センサー、最終要素	
	X_{LS}	Y_{LS}	X_{SF}	Y_{SF}
チャンネルは、異なる電気技術、例えば一つの電子機器又はプログラマブル電子機器又はリレーを使用しているか？	7.0			
チャンネルは、異なる電子技術、例えば一つの電子機器及び他のプログラマブル電子機器を使用しているか？	5.0			
デバイスは、センサー要素に対して異なった物理的な原理を使用しているか？（例えば、温度と圧力、ベーン風力計とドップラートランスデューサ）			7.5	
デバイスは、異なった電気的な原理/設計を採用しているか？（例えば、デジタルとアナログ、異なった製造業者又は異なったテクノロジー）			~~5.5~~	
チャンネルは MooN の高度冗長度を採用してい	2.0	0.5	2.0	0.5

るか。N＞M+2 か？				
チャンネルは MooN の高度冗長度を採用しているか。N＝M+2 か？	1.0	0.5	1.0	0.5
低度の多様性か？例えば、同じ技術を使用したハードウェアの診断試験	~~2.0~~	~~1.0~~		
中度の多様性か？例えば、異なる技術を使用したハードウェアの診断試験	3.0	1.5		
チャンネルは、異なる設計者によって情報交換することなく設計されたか？	~~1.0~~	~~1.0~~		
試運転中に別々の試験方法と人員が、各チャンネルに使用されたか？	~~1.0~~	~~0.5~~	~~1.0~~	~~1.0~~
保守は、異なった時間に別の人員によって行われたか？	~~2.5~~		~~2.5~~	

３．複雑さ/設計/用途/成熟度/経験

項　　目	論理回路		センサー、最終要素	
	X_{LS}	Y_{LS}	X_{SF}	Y_{SF}
チャンネル間の相互接続では、診断試験又はボーティングに使用される以外の情報交換が除外されているか？	~~0.5~~	~~0.5~~	~~0.5~~	~~0.5~~
設計は、５年を超えて現場で使用されてきた機器で使用された方法に基づいているか？	~~0.5~~	~~1.0~~	~~1.0~~	~~1.0~~
同じハードウェアを類似環境で使用した経験が５年を超えているか？	~~1.0~~	~~1.5~~	~~1.5~~	~~1.5~~
システムは単純か？例えば１チャンネルあたりの入力又は出力部は 10 個以下か？		1.0		
入力又は出力部は、発生しうる過電圧及び過電流から保護されているか？	~~1.5~~	~~0.5~~	~~1.5~~	~~0.5~~
全てのデバイス／構成要素は保守的な定格値になっているか？	~~2.0~~		~~2.0~~	

４．評価/データの解析とフィードバック

項　　目	論理回路		センサー、最終要素	
	X_{LS}	Y_{LS}	X_{SF}	Y_{SF}
FMEA 及びフォールトツリー解析の結果が検討されて、共通原因故障の源が明らかにされて共通原因故障の特定の源が設計によって除去されたか？		~~3.0~~		~~3.0~~
共通原因故障が設計の見直し時に考慮され、結果が設計にフィードバックされたか？（設計の見直し作業の証拠文書が要求される。）		~~3.0~~		~~3.0~~
現場での全ての故障が分析されて、フィードバックが設計になされているか？（手順の証拠文書が要求される。）	~~0.5~~	~~3.5~~	~~0.5~~	~~3.5~~

５．手順/インターフェース

項　　目	論理回路		センサー、最終要素	
	X_{LS}	Y_{LS}	X_{SF}	Y_{SF}
全ての構成要素故障（又は劣化）が検出され、根本原因が明らかにされて、他の類似項目が類似の潜在的な故障原因について検査されることを保証するシステム作業書があるか？		1.5	0.5	1.5
独立チャンネルの全ての部分の保守（調整や較正を含む）が計時的に行われ、保守に続いて実施される手動検査の他に、診断試験をあるチャンネルの保守の終了と他のチャンネルの保守の開始との間で首尾よく実施できるようにする手順が適切に準備されているか？	1.5	0.5	2.0	1.0
冗長系（例えばケーブル等）の全ての部分が互いに独立しているようにする、また、移動できないようにすることがプリント基板上などの保守は、全て現場外の認定修理センターでが実施され、修理したアイテムは全て完全な事前据付試験が実施されるか？	0.5	0.5	0.5	0.5
システムは、診断範囲が狭くて（60～90%）現場で交換可能なモジュールのレベルまで故障が報告されているか？	0.5	1.0	0.5	1.5
システムは、診断範囲が中位で（90～99%）現場で交換可能なモジュールのレベルまで故障が報告されているか？	0.5			
システムは、診断範囲が広くて（＞99%）現場で交換可能なモジュールのレベルまで故障が報告されているか？	1.5	1.0		
システムの診断試験では、現場で交換可能なモジュールのレベルまで故障が報告されているか？	2.5	1.5	1.0	1.0

６．コンピテンシー/訓練/安全文化

項　　目	論理回路		センサー、最終要素	
	X_{LS}	Y_{LS}	X_{SF}	Y_{SF}
設計者は共通原因故障の原因と結果を理解できるほどの訓練（文書化の訓練を含む）を受けているか？	2.0	3.0	2.0	3.0
保守要員は、共通原因故障の原因と結果を理解できるほどの訓練（文書化の訓練を含む）を受けているか？	0.5	4.5	0.5	4.5

７．環境のコントロール

項　　目	論理回路		センサー、最終要素	
	X_{LS}	Y_{LS}	X_{SF}	Y_{SF}
要員のアクセスは限定されているか（例えばキャビネットの施錠やアクセスできない場所）	0.5	2.5	0.5	2.5
システムは常に外部の環境制御装置を使用することなく試験済みの温度、湿度、腐食、埃、振動などの範囲内で運転されるようになっているか？	3.0	1.0	3.0	1.0
全ての信号・電源ケーブルは全ての場所で別々になっているか？	2.0	1.0	2.0	1.0

８．環境試験

項　　目	論理回路		センサー、最終要素	
	X_{LS}	Y_{LS}	X_{SF}	Y_{SF}
システムは関連する環境上の影響全て（例えば、EMC,温度、振動、衝撃、湿度）に対するイミュニティーに関して、認定規格で規定された適正レベルまで試験されているか？	10.0	10.0	10.0	10.0

以上より、Ｘ値とＹ値の集計値は表１１のようになる。

表１１　Ｓ値の評価結果

合計値	論理回路		センサー、最終要素	
	X_{LS}	Y_{LS}	X_{SF}	Y_{SF}
	43.5	45.5	39.5	41.5
	89		81	

〖ステップ２　診断試験間隔と診断率によるＺ値の決定〗

次に自己診断機能を有する場合には､表１２（第 6 部の表 D.2(プログラマブル電子機器)）と表１３（表 D.3（センサー又は最終要素））に従って診断試験間隔と診断率の程度によってＺ値を求めるが、本章の 2 重系の事例では運転中の自己診断は考慮していないので表１２と表１３は使用しない。

表１２（第 6 部表 D.2）Z 値：プログラマブル電子機器

診断率	診断試験間隔		
	1 分未満	1～5 分	5 分を超える
≧99%	2.0	1.0	0
≧90%	1.5	0.5	0
≧60%	1.0	0	0

表１３（第 6 部表 D.3）Z 値：センサー又は最終要素

診断率	診断試験間隔			
	2 時間以内	2 時間～2 日間	2 日間～1 週間	1 週間を超える
≧99%	2.0	1.5	1.0	0
≧90%	1.5	1.0	0.5	0
≧60%	1.0	0.5	0	0

以上をまとめると表１４になる。

表１４　S 値の評価結果

項目	論理回路（リレー）		センサー、最終要素（遮断弁）	
	X_{LS}	Y_{LS}	X_{SF}	Y_{SF}
	43.5	45.5	39.5	41.5
S=X+Y	89		81	
Z	-		-	
S_D=X(Z+1)+Y	-		-	

〖ステップ３　β又はβD の決定〗

次に S 値（又は S_D 値）によって表１（第 6 部表 D.4）からβ（又はβD）を求める。本事例では S 値によってβを求める。

表１５（第 6 部表 D.4）β又はβD

スコア（S 又は S_D）	β又はβD	
	論理回路（リレー）	センサー、最終要素（遮断弁）
120 超過	0.5%	1%
70～120	1%	2%
45～70	2%	5%
45 未満	5%	10%

リレーについては、S 値（S=X+Y）が 89 であるのでβが 1%。また、遮断弁については、S 値（S=X+Y）が 81 であるのでβは 2%になる。

３．２．２　低水位/燃焼系遮断の構成例（１）

ア　機能ブロック図

図１１は、低水位/燃焼系遮断の構成例（１）の機能ブロック図である。

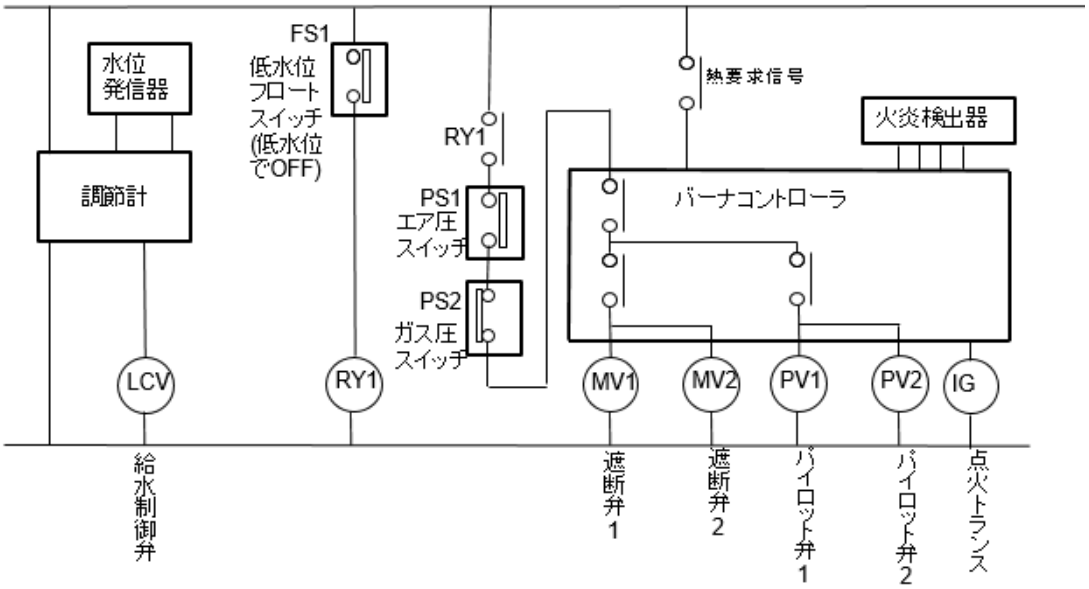


図１１　機能ブロック図　低水位/燃焼系遮断の構成例（１）

本図は、水位制御、燃焼制御の一例である。水位検出用発信器からの信号をうけて調節計にて給水制御弁を制御することで水位を制御し、バーナコントローラにて、各インターロックと火炎を監視し燃料遮断弁を制御している。これらの個別製品を組みあわて構成し、必要に応じて信号の受渡しにリレーを使用して設計している例である。
本図の例では、水位の異常低下や主バーナの異常失火に対して以下のように設計している。

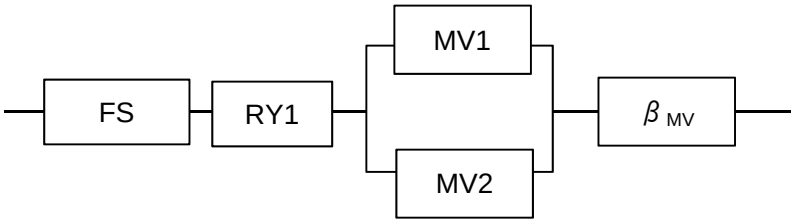
①危険事象：水位異常低下した場合の過熱/空焚きによる火災又は圧壊
　要求安全機能　：水位が安全低水位以下になった場合に燃料を遮断する
　入力　　：FS1 で安全低水位をチェック。安全低水位以上で接点 ON、安全低水位以下で接点 OFF。
　ロジック　　：リレーRY1 で遮断弁制御。なお、リレーRY1 の接点と遮断弁の間に、エア圧スイッチ接点・ガス圧スイッチ接点・バーナコントローラリレー接点が配置されているが、これらの接点は水位の異常低下の安全機能ロジックには関与していない。
　出力　　：遮断弁 MV1、MV2 を燃料配管に 2 個直列に設置
　診断/点検　　：FS1 は、作動確認を 3 日に 1 回実施する。火炎検出器は、24 時間に 1 回以上、バーナコントローラとのループで起動チェック(診断)される。遮断弁は、月に 1 回、漏れ点検(遮断機構の作動確認)する。
②危険事象：主バーナが異常失火した場合の燃料流出による爆発/火災
　要求安全機能　：火炎が異常失火した場合に燃料を遮断する
　入力　　：火炎検出器にて火炎監視(火炎信号)
　ロジック　　：バーナコントローラにて火炎有無判定・遮断弁制御
　出力　　：遮断弁 MV1、MV2 を燃料配管に 2 個直列に設置

診断/点検　　：火炎検出器は、24 時間に 1 回以上、バーナコントローラとのループで起動チェック(診断)される。遮断弁は、月に１回、漏れ点検(遮断機構の作動確認)する。

イ　危険事象：水位異常低下した場合の過熱/空焚きによる火災又は圧壊

（ア）信頼性ブロック図

図１１の機能ブロック図をもとにして作成した安全機能の信頼性ブロック図を図１２に示す。



ＦＳ；低水位スイッチ
ＲＹ１；リレー１
ＭＶ１；遮断弁１
ＭＶ２；遮断弁２
β_{MV}；遮断弁１、２の共通原因故障

図１２　信頼性ブロック図（１）

（イ）PFDavg の計算

図１２の機能ブロック図に示した構成要素の危険側故障率を表１６に示す。

表１６　構成要素の危険側故障率

記号	構成要素	λ_D危険側故障率（FIT）
ＦＳ	低水位スイッチ	500
ＲＹ１	リレー	2,000
ＭＶ１	遮断弁１	10,000
ＭＶ２	遮断弁２	10,000

注　例示のために故障率は任意の値としている。

各サブシステムの計算条件（想定値）と計算結果を表１７にまとめた。

表１７　サブシステムの計算条件と結果

項目	低水位スイッチ (FS)	リレー (RY1)	遮断弁 (MV1, MV2)
構成	1oo1	1oo1	1oo2
PFDGの計算式	(16)	(16)	(22)
危険側故障率 λ_D（FIT）注1	500	2000	10000
プルーフテスト間隔T_1 注2,注4	3日	1年	1か月
平均修理時間MRT(時間)	8	8	8
tCE （時間）	44.0	4388.0	373.0
tGE （時間）	−	−	251.3
β（%）　注3	−	−	2.0
PFDG	2.200E-05	8.776E-03	9.261E-05
SIL(相当値)	4	2	4

注1　計算では１時間あたりの故障数に換算する（$\times 10^{-9}$）。
注2　計算では時間に換算する。
注3　計算では少数に換算する（×0.01）。
注４　プルーフテスト間隔は図１１より以下のように設定した。
　　低水位スイッチ；3 日
　　リレー；　１年
　　遮断弁；　１か月

運転中の診断はないとしたので、遮断弁の診断による共通原因故障割合β_Dは表から削除している。

（ランダムハードウェア故障確率）

PFDavg = 2.200E-5 + 8.776E-3 + 9.261E-5 = 8.891E-3

この PFDavg は、SIL2 になる。

（ウ）アーキテクチャ制約

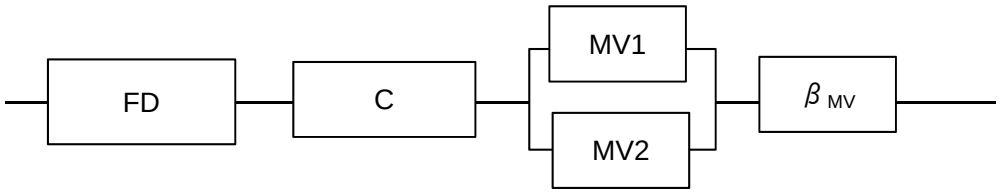
システムのアーキテクチャ制約の要求により、最小の SIL を有するサブシステムの SIL によってシステム全体の SIL が制約される
ランダムハードウェア故障確率の計算からはシステム全体の SIL は 2 であり、かつ、表１７からは、リレーの SIL2 によって制約されて全体システムの SIL は 2 になる。

従って、ランダムハードウェア故障確率計算とアーキテクチャ制約の検討から、システムは SIL2 となる。

ウ　危険事象：バーナの異常失火した場合の燃料流出による爆発/火災

（ア） 信頼性ブロック図

信頼性ブロック図を図１３に示す。



ＦＤ；火炎検出器
Ｃ；コントローラ
ＭＶ１；遮断弁１
ＭＶ２；遮断弁２
β_{MV}；遮断弁１、２の共通原因故障

図１３　信頼性ブロック図（２）

（イ）PFDavg の計算

それぞれが同じ要素である遮断弁（MV1 と MV2）の共通原因故障割合β_{MV}を考慮した。

図１３の機能ブロック図に示した構成要素の危険側故障率を表１８に示す。

表１８　構成要素の危険側故障率

記号	構成要素	λ_D危険側故障率（FIT）
ＦＤ	火炎検出器	40,000
Ｃ	コントローラ	300
ＭＶ１	遮断弁１	10,000
ＭＶ２	遮断弁２	10,000

注　例示のために故障率は任意の値としている。

各サブシステムの計算条件と計算結果を表１９に示した。

表１９　サブシステムの計算条件と結果

項目	火炎検出器 (FD)	コントローラ (C)	遮断弁 (MV1,MV2)
構成	1oo1	1oo1	1oo2
PFDGの計算式	(16)	(16)	(22)
危険側故障率λD (FIT) 注1	40000	300	10000
プルーフテスト間隔T_1　注2,注4	24時間	24時間	1か月
平均修理時間MRT(時間)	8	8	8
tCE (時間)	20.0	20.0	373.0
tGE (時間)	-	-	251.3
β(%) 注3	-	-	2.0
PFDG	8.000E-04	6.000E-06	9.261E-05
SIL(相当値)	3	<4	4

注1　計算では１時間あたりの故障数に換算する（$\times 10^{-9}$)。
注2　計算では時間に換算する。
注3　計算では少数に換算する（×0.01)。
注４　プルーフテスト間隔は図１１より以下のように設定した。
火炎検出器；24 時間
コントローラ；24 時間
遮断弁；　1 か月

運転中の診断はないとしたので、診断率 DC と遮断弁の診断による共通原因故障割合β_Dは表から削除している。

（ランダムハードウェア故障確率）

PFDavg = 8.000E-4 + 6.000E-6 + 9.261E-5　=　8.986E-4

この PFDavg は、表１９より、SIL3 となる。

（ウ）アーキテクチャ制約

ランダムハードウェア故障確率の計算からはシステム全体の SIL は 3 であり、かつ、表１９から、火炎検出器の SIL3 によって制約されて全体システムの SIL は 3 になる。

従って、ランダムハードウェア故障確率計算とアーキテクチャ制約の両者からシステムは SIL3 となる。

３．２．３　低水位/燃焼系遮断の構成例（２）

ア　機能ブロック図

図１４は、低水位/燃焼系遮断の構成例（２）の機能ブロック図である。

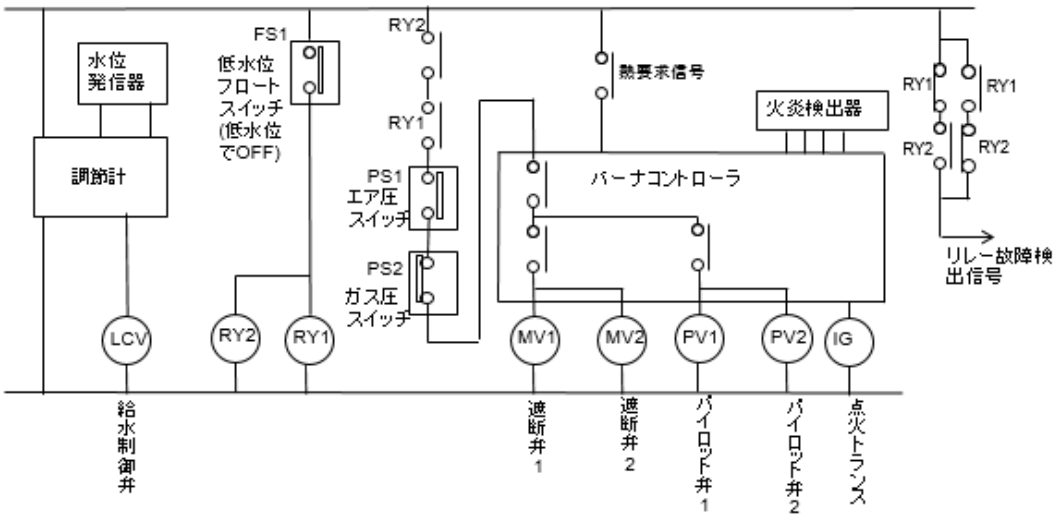


図１４　機能ブロック図　低水位/燃焼系遮断の構成例（２）

低水位遮断機能：
RY1、RY2 のどちらかが OFF できれば遮断弁が OFF できる。(2 重化)
(注:接点溶着が危険側故障)

RY1,RY2 の診断機能：
ボイラー点検時に低水位発生させて(水を抜いて)遮断できるか確認した時に、RY1,RY2 のどちらかの接点が溶着していると診断出力が ON。
(注；この診断がないと低水位機能作動の点検をしたときに、どちらかひとつのリレーが溶着していても分からない)

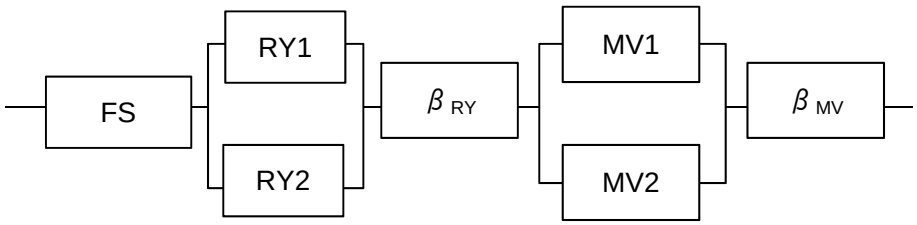
低水位/燃焼系遮断の構成例（１）に加えて、リレーが２重化（ＲＹ１、ＲＹ２）され、かつ、リレー故障の検出回路によって故障を検出した場合には、リレーを交換するように改良されている。

火炎検出器の診断機能：
火炎検出器は構成例（１）では、24 時間に 1 回以上、バーナコントローラとのループで起動チェック(診断)されるが、構成例（２）では自己診断機能により火炎検出器が故障していないか、シャッターにより光感知部を２秒に １ 度、定期的に遮断し、火炎検出器自身が自己診断を実施する。故障を検知すると遮断弁が閉じられる。

イ　危険事象：水位異常低下した場合の過熱/空焚きによる火災又は圧壊

（ア）信頼性ブロック図

信頼性ブロック図を図１５に示す。



ＦＳ；低水位スイッチ
ＲＹ１；リレー１
ＲＹ２；リレー２
ＭＶ１；遮断弁１
ＭＶ２；遮断弁２
β_{RY}；リレー１、２の共通原因故障割合
β_{MV}；遮断弁１、２の共通原因故障割合

図１５　信頼性ブロック図（３）

（イ）PFDavg の計算

図１５の信頼性ブロック図に示した構成要素の危険側故障率を表２０に示す。

表２０　構成要素の危険側故障率

記号	構成要素	λ_D危険側故障率（FIT）
ＦＳ	低水位スイッチ	500
ＲＹ１	リレー	2,000
ＲＹ２	リレー	2,000
ＭＶ１	遮断弁１	10,000
ＭＶ２	遮断弁２	10,000

注　例示のために故障率は任意の値としている。

各サブシステムの計算条件と計算結果を表２１にまとめた。

表２１　サブシステムの計算条件と結果

項目	低水位スイッチ (FS)	リレー (RY1, RY2)	遮断弁 (MV1, MV2)
構成	1oo1	1oo2	1oo2
PFDGの計算式	(16)	(22)	(22)
危険側故障率 λ_D（FIT）注1	500	2000	10000
プルーフテスト間隔T_1 注2,注4	3日	1年	1か月
平均修理時間MRT(時間)	8	8	8
tCE （時間）	44.0	4388.0	373.0
tGE （時間）	－	2928.0	251.3
β（%） 注3	－	1.0	2.0
PFDG	2.200E-05	1.885E-04	9.261E-05
SIL(相当値)	4	3	4

注１　計算では１時間あたりの故障数に換算する（$\times 10^{-9}$）。
注２　計算では時間に換算する。
注３　計算では少数に換算する（×0.01）。
注４　プルーフテスト間隔は図１４より以下のように設定した。
　　低水位スイッチ；3 日
　　リレー；　1 年
　　遮断弁；　1 か月

（ランダムハードウェア故障確率）
PFDavg = 2.200E-5 + 1.885E-4 + 9.261E-5　＝　3.031E-4

この PFDavg は SIL3 となる。

（ウ）アーキテクチャ制約

ランダムハードウェア故障確率の計算からはシステム全体の SIL は 3 であり、かつ、表２１から、リレーの SIL3 に制約されて全体システムの SIL は 3 になる。

従って、ランダムハードウェア故障確率計算とアーキテクチャ制約の両者から、システムは SIL3 となる。

ウ　危険事象：バーナの異常失火した場合の燃料流出による爆発/火災

（ア）信頼性ブロック図

信頼性ブロック図は、図１３と同一である。

（イ）PFDavg の計算

構成要素の危険側故障率は表１８と同一である。

各サブシステムの計算条件と計算結果を表２２に示した。表２２では、火炎検出器以外は表１９と同一である。

表２２　サブシステムの計算条件と結果

項目	火炎検出器 (FD)	コントローラ (C)	遮断弁 (MV1,MV2)
構成	1oo1	1oo1	1oo2
PFDGの計算式	(20)	(16)	(22)
危険側故障率λ_D（FIT） 注1	40000	300	10000
診断率 DC　注５	0.6	-	-
検知不可危険側故障率λ_{DU}（FIT） 注1	16000	-	-
検知可能危険側故障率λ_{DD}（FIT） 注1	24000	-	-
プルーフテスト間隔T_1　注2,注4	24時間	24時間	1か月
平均修復時間MTTR(時間)	8	-	-
平均修理時間MRT(時間)	8	8	8
tCE （時間）	12.8	20.0	373.0
tGE （時間）	-	-	251.3
β（%） 注3	-	-	2.0
PFDG	2.048E-04	6.000E-06	9.261E-05
SIL(相当値)	3	<4	4

注１　計算では 1 時間あたりの故障数に換算する（$\times 10^{-9}$）。
注２　計算では時間に換算する。
注３　計算では少数に換算する（×0.01）。
注４　プルーフテスト間隔は図 14 より以下のように設定した。
　　火炎検出器；24 時間
　　コントローラ；24 時間
　　遮断弁；　1 か月
注５　火炎検出器のシャッターによる診断率は、IEC 61508 第 2 部付属書 A 表 A.13、センサーの「オンライン監視による故障検出」の低頻度モードの診断率から診断率低（≧60%）とした。なお、付録２　診断率（EN 13611:2007）では、診断率は 90%となっているが、診断率低の診断率は、IEC 61508 第 2 部付属書 A、A.2 注 2 の定義（診断率低：60%、診断率中：90%、診断率高：99%）から 60%とした。
なお、運転中の自己診断で検知できなかった故障は、24 時間毎のプルーフテストで完全に検知できるものとした。

火炎検出器については（２０）式によって PFDavg を計算した。.

（ランダムハードウェア故障確率）

PFDavg = 2.048E-4 + 6.000E-6 + 9.261E-5　=　3.034E-4

この PFDavg は、SIL3 となる。

（ウ）アーキテクチャ制約

ランダムハードウェア故障確率の計算からはシステム全体の SIL は 3 であり、かつ、表２２から、火炎検出器の SIL3 によって制約されて全体システムの SIL は 3 になる。

従って、ランダムハードウェア故障確率計算とアーキテクチャ制約の両者からシステムは SIL3 となる。

３．２．４　低水位/燃焼系遮断の構成例（３）

ア　機能ブロック図

図１６は、低水位/燃焼系遮断の構成例（３）の機能ブロック図である。

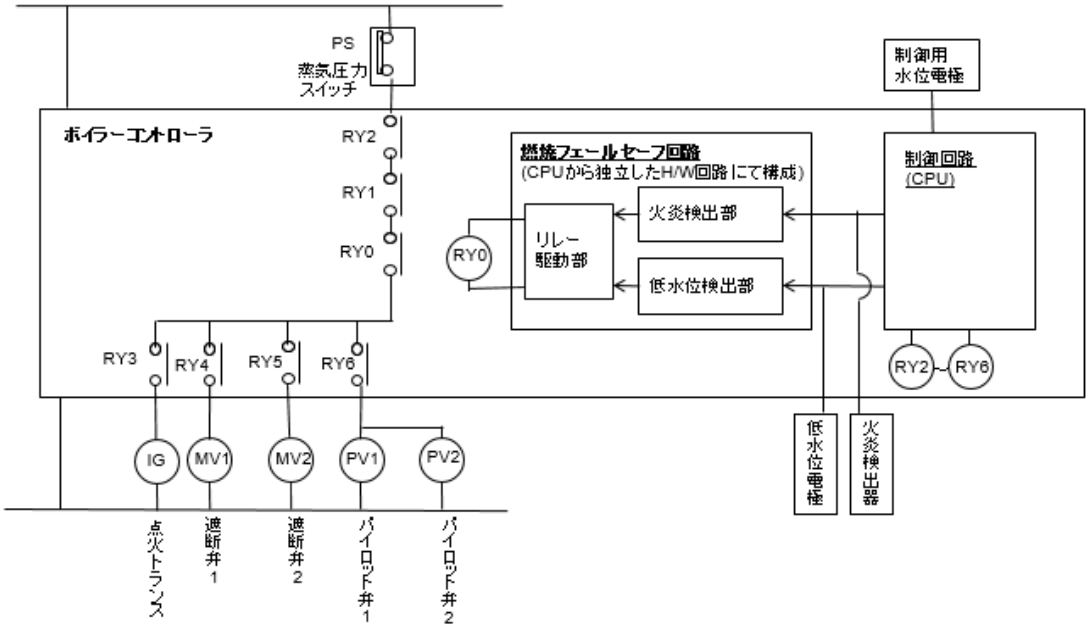


図１６　機能ブロック図　低水位/燃焼系遮断の構成例（３）

本図は、小型ボイラーなどで使用されているボイラーコントローラで構成した例である。このボイラーコントローラの例では、CPU を使用して構成されているボイラーの制御回路部と、CPU を使用せず独立したハードウェアで構成されている燃焼フェールセーフ回路が実装されている。燃焼フェールセーフ回路は、CPU の影響を受けずに作動する構成としており、本図の例では、水位の異常低下や主バーナの異常失火に対して以下のように設計している。

①危険事象：水位異常低下した場合の過熱/空焚きによる火災又は圧壊
　要求安全機能　：水位が安全低水位以下になった場合に燃料を遮断する
　入力　　：低水位電極で安全低水位をチェック。安全低水位異常で電極導通、安全低水位以下で電極非導通
　ロジック　　：燃焼フェールセーフ回路、RY0 で遮断弁制御。(RY4,RY5 は CPU で制御されるリレーで、この安全機能ロジックには関与しない)
　出力　　：遮断弁 MV1、MV2 を燃料配管に 2 個直列に設置
　診断/点検　　：水位電極は、24 時間に 1 回以上、燃焼フェールセーフ回路とのループで起動チェック(診断)される。遮断弁は、月に 1 回、漏れ点検(遮断機構の作動確認)する。

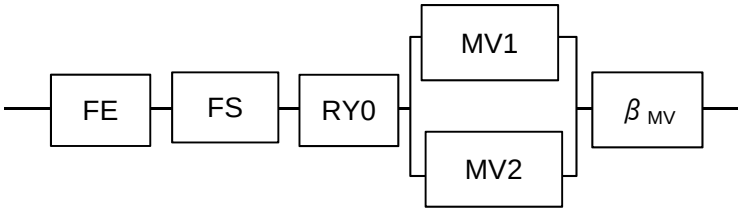
②危険事象：主バーナが異常失火した場合の燃料流出による爆発/火災
　要求安全機能　：火炎が異常失火した場合に燃料を遮断する
　入力　　：火炎検出器にて火炎監視(火炎信号)

ロジック　　：燃焼フェールセーフ回路、RY0 で遮断弁制御。(RY4,RY5 は CPU で制御されるリレーでこの安全機能ロジックには関与しない)
出力　　：遮断弁 MV1、MV2 を燃料配管に 2 個直列に設置
診断/点検　　：火炎検出器は、24 時間に 1 回以上、燃焼フェールセーフ回路とのループで起動チェック(診断)される。遮断弁は、月に１回、漏れ点検(遮断機構の作動確認)する。

イ　危険事象：水位異常低下した場合の過熱/空焚きによる火災又は圧壊

（ア） 信頼性ブロック図

信頼性ブロック図を図１７に示す。



ＦＥ；低水位電極
ＦＳ；燃焼フェールセーフ回路
ＲＹ０；リレー
ＭＶ１；遮断弁１
ＭＶ２；遮断弁２
β_{MV}；遮断弁１と遮断弁２の共通原因故障割合

図１７　信頼性ブロック図（５）

（イ）PFDavg の計算

① 危険事象：水位異常低下した場合の過熱/空焚きによる火災又は圧壊

機能ブロック図に示した構成要素の危険側故障率を表２３に示す。

表２３　構成要素の危険側故障率

記号	構成要素	λ_D危険側故障率（FIT）
ＦＥ	低水位電極	3,500
ＦＳ	燃焼フェールセーフ回路	10,000
ＲＹ０	リレー	2,000
ＭＶ１	遮断弁１	10,000
ＭＶ２	遮断弁２	10,000

注　例示のために故障率は任意の値としている。

各サブシステムの計算条件と計算結果を表２４にまとめた。

表２４　サブシステムの計算条件と結果

項目	低水位電極 (FE)	燃焼フェールセーフ回路	リレー (RY0)	遮断弁 (MV1,MV2)
構成	1oo1	1oo1	1oo1	1oo2
PFDGの計算式	(16)	(16)	(16)	(22)
危険側故障率λ_D（FIT） 注1	3500	10000	2000	10000
プルーフテスト間隔T_1 注2,注4	24時間	24時間	1年	1か月
平均修理時間MRT(時間)	8	8	8	8
tCE （時間）	20.0	20.0	4388.0	373.0
tGE （時間）	-	-	-	251.3
β（%） 注3	-	-	-	2.0
PFDG	7.000E-05	2.000E-04	8.776E-03	9.261E-05
SIL(相当値)	4	3	2	4

注１　計算では１時間あたりの故障数に換算する（$\times 10^{-9}$)。
注２　計算では時間に換算する（×8760)。
注３　計算では少数に換算する（×0.01)。
注４　プルーフテスト間隔は図１６より以下のように設定した。
低水位スイッチ；24 時間
燃焼低フェールセーフ回路；24 時間
リレー；　1 年
遮断弁；　1 か月

（ランダムハードウェア故障確率）

PFDavg = 7.000E-5 + 2.000E-4 + 8.776E-3 + 9.261E-5　=
9.139E-3

この PFDavg は SIL2 となる。

（ウ）アーキテクチャ制約

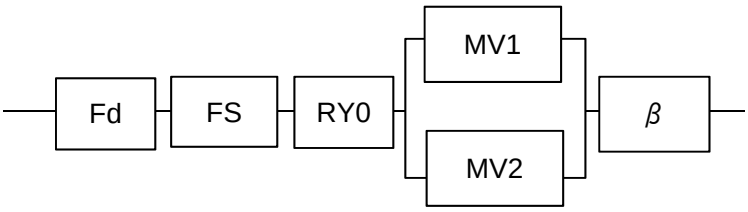
ランダムハードウェア故障確率の計算からはシステム全体の SIL は 2 であり、かつ、表２４から、リレーの SIL2 によって制約されて全体システムの SIL は 2 になる。

従って、ランダムハードウェア故障確率計算とアーキテクチャ制約からシステムは SIL2 となる。

ウ　危険事象：主バーナが異常失火した場合の燃料流出による爆発/火災

（ア）信頼性ブロック図

信頼性ブロック図を図１８に示す。



Ｆｄ；火炎検出器
ＦＳ；燃焼フェールセーフ回路
ＲＹ０；リレー１
ＭＶ１；遮断弁１
ＭＶ２；遮断弁２
β_{MV}；遮断弁１と遮断弁２の共通原因故障割合

図１８　信頼性ブロック図（６）

（イ）PFDavg の計算

機能ブロック図に示した構成要素の危険側故障率を表２５に示す。

表２５　構成要素の危険側故障率

記号	構成要素	λ_D危険側故障率（FIT）
Ｆｄ	火炎検出器	40,000
ＦＳ	燃焼フェールセーフ回路	10,000
ＲＹ０	リレー	2,000
ＭＶ１	遮断弁１	10,000
ＭＶ２	遮断弁２	10,000

注　例示のために故障率は任意の値としている。
燃焼フェールセーフ回路については、ＦＭＥＤＡによって故障分析が実施されているものとする。認証された製品であれば、ＦＭＥＤＡの評価レポートや安全マニュアルから必要な故障率を入手する。

各サブシステムの計算条件と計算結果を表２６にまとめた。

表２６　サブシステムの計算条件と結果

項目	火炎検出器 (Fd)	燃焼フェールセーフ回路	リレー (RY0)	遮断弁 (MV1,MV2)
構成	1oo1	1oo1	1oo1	1oo2
PFDGの計算式	(16)	(16)	(16)	(22)
危険側故障率λD（FIT）注1	40000	11000	2000	10000
プルーフテスト間隔T_1 注2,注4	24時間	24時間	1年	1か月
平均修理時間MRT(時間)	8	8	8	8
tCE（時間）	20.0	20.0	4388.0	373.0
tGE（時間）	-	-	-	251.3
β(%) 注3	-	-	-	2.0
PFDG	8.000E-04	2.200E-04	8.776E-03	9.261E-05
SIL(相当値)	3	3	2	4

注１　計算では１時間あたりの故障数に換算する（$\times 10^{-9}$)。

注２　計算では時間に換算する。

注３　計算では少数に換算する（×0.01)。

注４　プルーフテスト間隔は図１６より以下のように設定した。

火炎検出器；24 時間（0.0027 年）

燃焼フェールセーフ回路；24 時間

リレー；　1 年

遮断弁；　1 か月

（ランダムハードウェア故障確率）

PFDavg =　8.000E-4 + 2.200E-4 +　8.776E-3 + 9.261E-5

=　9.889E-3

この PFDavg は SIL2 となる。

（ウ）アーキテクチャ制約

ランダムハードウェア故障確率の計算からはシステム全体の SIL は 2 であり、かつ、表２６から、リレーの SIL2 によって制約されて全体システムの SIL は 2 になる。

従って、ランダムハードウェア故障確率計算とアーキテクチャ制約からシステムは SIL2 となる。

ウ　安全機能間の共有

構成例（３）においては、①危険事象：水位異常低下した場合の過熱/空焚きによる火災又は圧壊に対する安全機能と、②危険事象：主バーナが異常失火した場合の燃料流出による爆発/火災に対する安全機能の間に燃焼フェールセーフ回路のリレー駆動部（RYA）とリレー（RY0）が共有されている。

IEC 61508 第 2 部 7.4.2.4 より、異なる安全度水準（SIL）の安全機能が分離されていない場合には、高い安全度水準（SIL）の場合の要求事項が適用されることに注意する必要がある。
ただし、本構成例の場合、両者が SIL2 であるので SIL2 の要求事項に適合すればよいことになる。

３．２．５　まとめ

以上の低水位/燃焼系遮断の構成例について安全機能のＳＩＬの評価結果を表２７にまとめた。

表２７　ＳＩＬ評価結果のまとめ

危険事象	水位異常低下した場合の過熱/空焚きによる火災又は圧壊	主バーナが異常失火した場合の燃料流出による爆発/火災
構成例（１）	ＳＩＬ２	ＳＩＬ３
構成例（２）	ＳＩＬ３	ＳＩＬ３
構成例（３）	ＳＩＬ２	ＳＩＬ２

第４章　妥当性確認

１．　はじめに

本章では、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（機能安全指針）に基づき、設計製造されたボイラー制御系の機能安全妥当性確認の手順とそれに必要な資料について述べる。

２．　妥当性確認

妥当性確認とは、IEC 61508-1 の図 2（全安全ライフサイクル)、及び、表 1（全安全ライフサイクル：概要）に示される該当するボックス毎に当初計画されたプロトコル通りに実施されたことを必要な資料で確認することであり、IEC 61508 シリーズの次の条項により規定されている。(注[1])

① 全安全ライフサイクル（IEC 61508-1　7.1)、

② 電子等制御ライフサイクル（IEC 61508-2　7.7）及び

③ ソフトウェアライフサイクル（IEC 61508-3　7.7）

前記①～③について、対象システム、又は、システムを構成する部品の妥当性確認プロセスを図 4-1、4-2 のフロー、及び、表 4-1 に示す。

2.1 ソフトウェアライフサイクル

ソフトウェアについては、IEC 61508-3 の 7.7 項に従い次のように実施する必要がある（表 4-1 のボックス 10)。

(1) 妥当性確認業務は、ソフトウェアに関する妥当性確認計画に規定するとおりに実施すること。

(2) ソフトウェア開発の性質に応じて、IEC 61508 -3 の 7.7 項 への適合責任は複数の当事者が負うことがあるので、責任分担は、安全計画時に文書化しておくこと。（IEC 61508-1 の 6 項 参照）。

(3) システム安全のソフトウェアの妥当性確認結果は、文書化すること。

(4) ソフトウェア安全妥当性確認では、安全機能別に、次の結果を文書化しなければならない。

① 業務のシーケンスを遡及できるようにする、妥当性確認業務の経時的記録

② 使用するシステム安全のソフトウェアの妥当性確認計画のバージョン

③（テスト又は解析によって）妥当性確認する安全機能と合わせて、システム安全のソフトウェアの妥当性確認計画の参照

（注[1]）必要な資料の作成とまとめ方については、JIS Q 17050-1 (（適合性評価一供給者適合宣言-第 1 部: 一般要求事項)、及び、JISQ17050-2（適合性評価一供給者適合宣言-第 2 部: 支援文書）を参照することを推奨する。

④　校正データ、並びに校正に使用するツール及び機器

⑤　妥当性確認業務の結果

⑥　予想結果と実際の結果との不整合

(5)　予想結果と実際の結果との不整合が生じた場合、妥当性確認を続けるか、又は変更要請を出して開発ライフサイクルの前の段階に戻るかどうかに関して行った解析及び決定事項を、システム安全のソフトウェア妥当性確認結果の一部として、文書化しなければならない。

(6)　システム安全の安全関連ソフトウェアの妥当性確認は、次の要求事項を満たさなければならない。

①　テストは、ソフトウェアの主要な妥当性確認法でなければならない。妥当性確認業務を補足するために、解析、アニメーション及びモデリングを用いてもよい。

②　ソフトウェアは、次のシミュレーションによって実行しなければならない。

ア）通常動作時に出る入力信号

イ）予想する事象

ウ）システム動作を要求する望ましくない状態

③　サプライヤ及び／又は開発者（若しくは適合性に責任を負う複数の当事者）は、製品が及び IEC 61508-2 の要求事項を満たすことができるように、システム安全のソフトウェアの妥当性確認に関する文書化した結果、及び全ての関連文書を、システム開発者に提供しなければならない。

(7)　ソフトウェアツールは、IEC 6508-3　7.4.4 項 の要求事項を満たさなければならない。

(8)　システム安全の安全関連ソフトウェアの妥当性確認結果は、次の要求事項を満たさなければならない。

①　テストは、規定した安全関連ソフトウェアの全ての安全要求仕様（IEC 6508-3 7.2 項 参照）を正確に満たし、ソフトウェアが想定外の機能を実行することがないことを示さなければならない。

②　テストケース及びそれらの結果は、安全度水準が要求する以降の解析及び独立した評価（IEC 6508-1　8 項 参照）用に文書化しなければならない。

③　システム安全のソフトウェアの妥当性確認結果を示す文書には、ソフトウェアが妥当性確認に合格したか、又は妥当性確認に不合格となった理由のいずれかを、明記しなければならない。

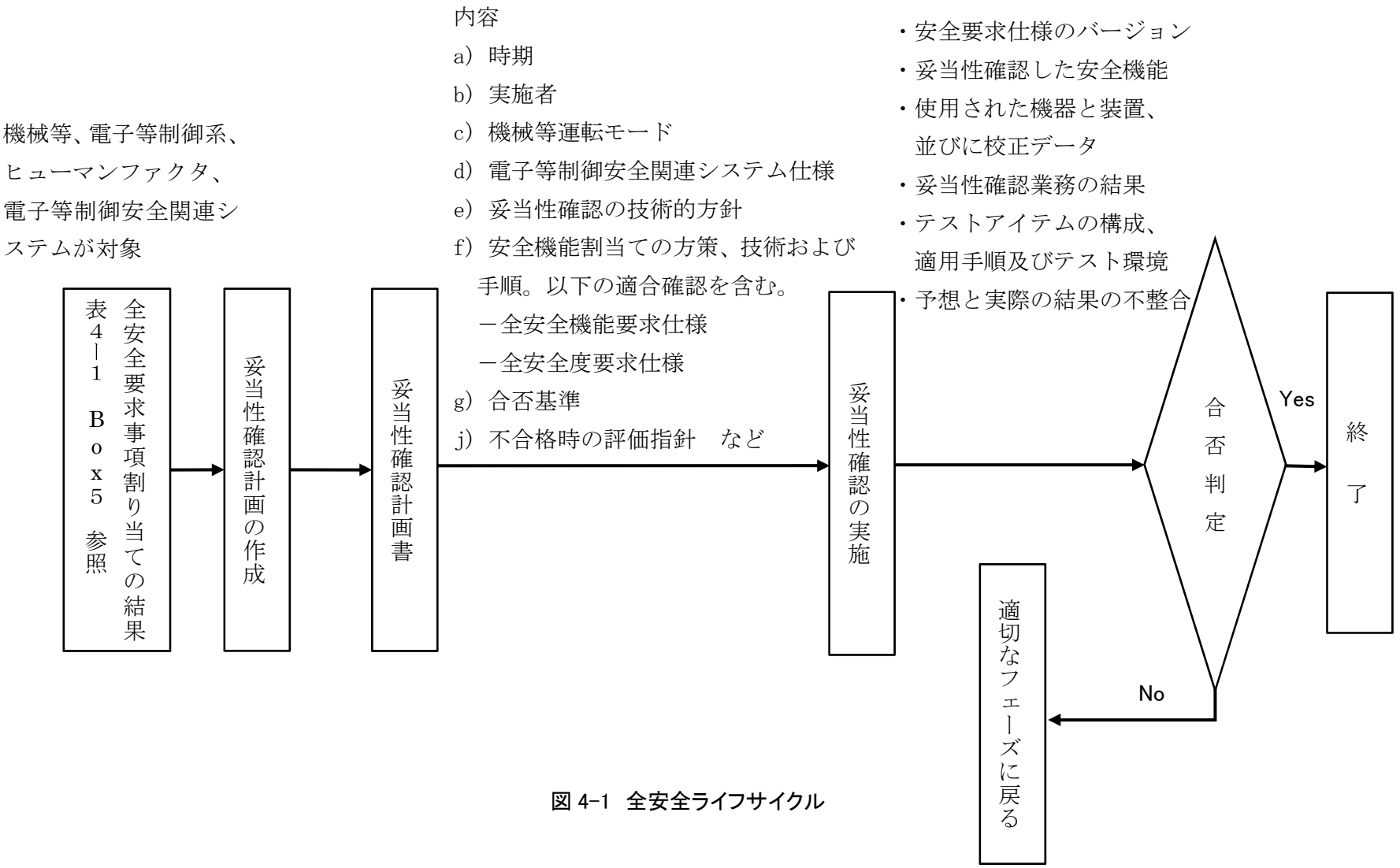


図 4-1　全安全ライフサイクル

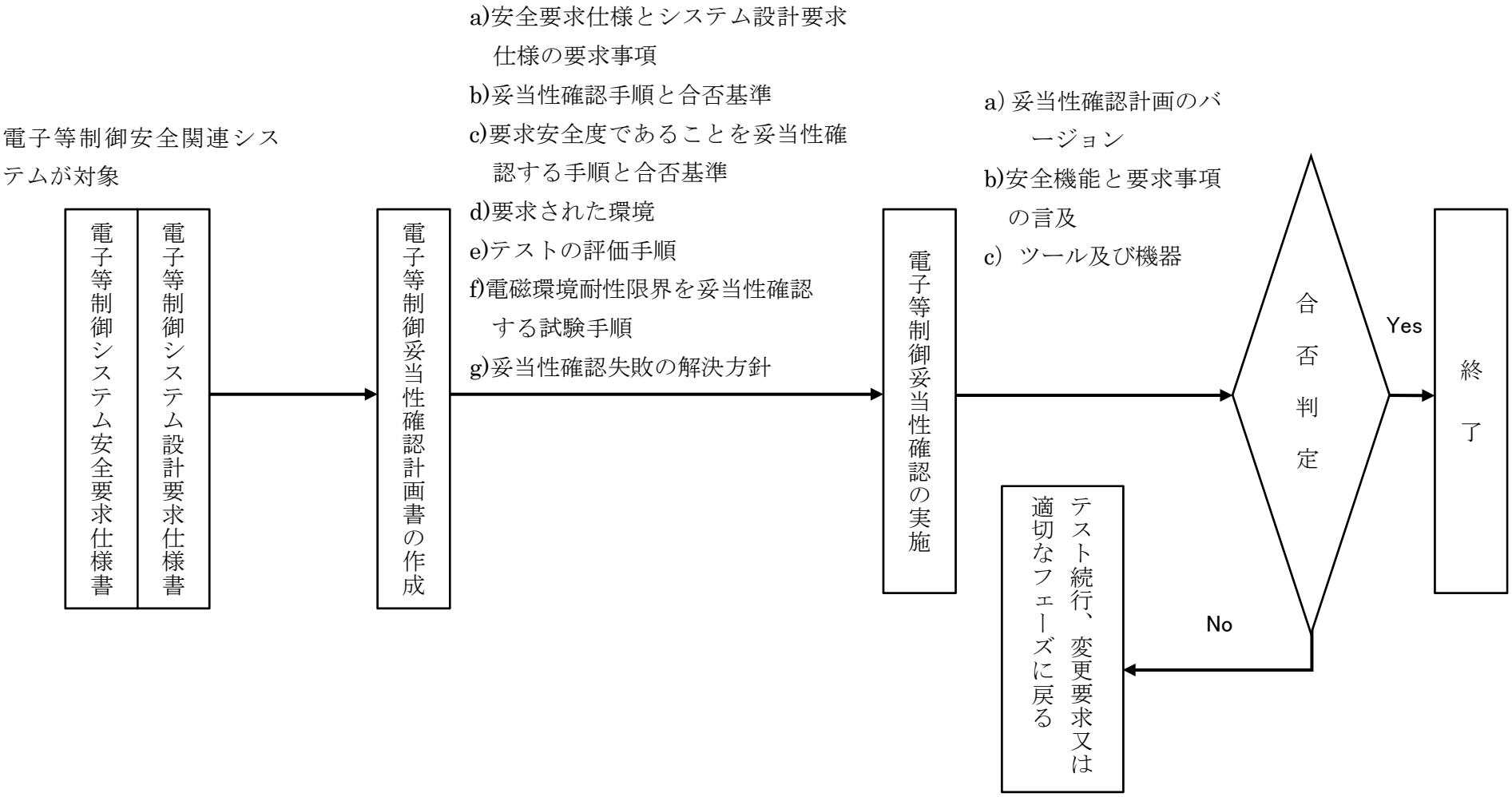


図 4-2 電子等制御ライフサイクル

表 4-1 全安全ライフサイクルにおける必要な書類リスト

JIS C 0508-1:2012 (IEC 61508-1 2010) 表 1 全安全ライフサイクルフェーズ:概要 より			妥当性確認に必要な資料など	
同規格図 2 の Box No.	表題		必要書類	項目例
1	概念	Part 1 の 7.2.1 項 他の安全ライフサイクル業務が十分に実行できるように被制御機器（以下、機械等）及びその環境（物理的、法的など）を一定水準まで理解する。 Part 2 の 7.2 項 設計要求事項の規定	設計仕様書	① 使用環 ② ユーティリティ ③ 使用条件 ④ 制限事項（耐用年数、MTTR、プルーフテストの条件） など
2	全対象範囲の定義	Part 1 の 7.3.1 項 機械等と 機械等 制御系との境界を明確化する。 潜在危険及びリスク解析（プロセス潜在危険、環境潜在危険など）の範囲を指定する。		
3	潜在危険及びリスク解析	Part 1 の 7.4.1 項 フォールト状態又は合理的に予見可能な誤使用を含む全ての合理的な予見可能状況で、機械等及び機械等制御系の潜在危険、危険状態及び危険事象を全ての運転モードで明確化する。 危険事象に導く事象連鎖を明らかにする。 危険事象に関連する 機械等 リスクを明らかにする。	リスクアセスメントシート	リスクアセスメントシート例参照
4	全安全要求事項	Part 1 の 7.5.1 項 必要な機能安全を達成するために、電子等制御 安全関連系、他リスク軽減措置に対して、全ての安全機能及び安全度要求事項に関わる仕様を展開する。	安全要求仕様書	安全状態の定義
5	全安全要求事項の割当て	Part 1 の 7.6.1 項 当該 電子等制御安全関連系に対して全安全要求仕様（安全機能及び安全度要求事項）に含まれる安全機能を割り当てる。 電子等制御安全関連系によって実施される各安全機能に安全度水準を割り当てる。	①ランダムハードウェア故障 ② 決定論的原因故障の回避	① FMEDA ② 評価計画
6	全運用及び保全計画	Part 1 の 7.7.1 項 電子等制御安全関連系の運用及び保全の間必要な機能安全の維持を保証	取扱説明書など	

JIS C 0508-1:2012 (IEC 61508-1 2010) 表 1 全安全ライフサイクルフェーズ:概要 より			妥当性確認に必要な資料など	
同規格図 2 の Box No.	表題		必要書類	項目例
		する目的で運用及び保全の計画を作成する。		
7	全安全妥当性確認計画	Part 1 の 7.8.1 項 電子等制御安全関連系の全安全妥当性確認を行う計画を作成する。 Part 2 の 7.3.(電子等制御系安全妥当性確認計画) 電子等制御 系設計及び開発と並行して実施する	妥当性確認計画書 試験計画、合否判定基準	
8	全設置及び引渡し計画	Part 1 の 7.9.1 項 要求される機能安全が達成できるよう、統御された方法で 電子等制御 安全関連系を設置するための計画を作成する。 要求される機能安全が達成できるよう、統御された方法で 電子等制御 安全関連系を引き渡すための計画を作成する。	契約書など	
9	電子等制御系安全要求仕様	Part 1 の 7.10.1 項 電子等制御安全機能要求仕様及び安全度要求事項の観点から、要求される機能安全を達成できるように 電子等制御 安全関連系の安全要求事項を定義する。	安全要求仕様書	
10	電子等制御安全関連系:実現	Part 1 の 7.11.1 項 この規格群の第 2 部及び第 3 部電子等制御安全関連系の安全要求事項に適合する電子等制御安全関連系の生成(電子等制御 機能要求事項仕様及び安全度要求事項仕様から成る)。 Part 3 の 7.7 項 統合したシステムが、要求安全度水準で、ソフトウェア安全要求仕様に必ず適合するようにすることである。 Part 3 の附属書 A と B	図面類 試験結果など	・系の適用範囲(型式などによる特定) ・系の動作説明 ・構造図、電気回路ブロック図、回路図、使用部品リスト

JIS C 0508-1:2012 (IEC 61508-1 2010) 表 1　全安全ライフサイクルフェーズ:概要　より			妥当性確認に必要な資料など	
同規格図 2 の Box No.	表題		必要書類	項目例
11	他リスク軽減措置:仕様及び実現	Part 1 の 7.12.1 項 安全機能要求及び安全度要求事項に適合する、他リスク軽減措置の生成（この規格群の適用範囲外）	適用外	ー
12	全設置及び引渡し	Part 1 の 7.13.1 項 電子等制御安全関連系を設置する。 電子等制御安全関連系を引き渡す。	・契約書 ・取扱説明書 ・手順書 など	設置者と使用者間の役割分担
13	全安全妥当性確認	Part 1 の 7.14.1 項 7.6 に従って展開された電子等制御安全関連系に対する安全要求事項の割当てを計算に入れて、全安全機能要求事項及び全安全度要求事項の形式による全安全要求仕様に、当該電子等制御安全関連系が適合していることを確認する。	妥当性確認計画書	
14	全運用、保全及び修理	Part 1 の 7.15.1 項 電子等制御安全関連系の機能安全を規定の水準に確実に保つ。 電子等制御安全関連系の運用、保全及び修理に必要とされる技術要求が、電子等制御安全関連系の将来的な保守運用責任者に確実に提供される。	・取扱説明書 ・手順書 など	
15	全部分改修及び改造	Part 1 の 7.16.1 項 部分改修及び改造が行われている間とその後で、電子等制御安全関連系に関わる機能安全が適切であることを確実にするために必要な手順を定義する。	・取扱説明書 ・手順書 など	
16	使用終了又は廃却	Part 1 の 7.17.1 項 機械等の使用終了又は廃却の間とその後で、電子等制御安全関連系の機能安全が適切であることを確実にするために必要な手順を定義する。	・取扱説明書 ・手順書 など	

第５章　適合性証明

１　はじめに

第三者による適合性証明には、製造者自身が第４章で実施された妥当性確認を行い、その結果をもとに供給者適合宣言を行うことになる。供給者適合宣言をもって適合性証明申請を行うことになるが、本章では、供給者適合宣言から適合性証明取得までの手順について述べる。

2.　参考文書

JIS Q 17050-1 (ISO/IEC 17050-1)適合性評価 供給者適合宣言 第 1 部：一般要求事項

JIS Q 17050-2 (ISO/IEC 17050-2)適合性評価 供給者適合宣言 第 2 部：支援文書

JIS Q 17065 (ISO/IEC 17065) 適合性評価–製品、プロセス及びサービスの認証を行う機関に対する要求事項

３　定義

3.1 供給者

対象品の品質責任を負う第一者。

3.2 申請者

対象品を登録適合証明機関に適合性証明の申請を行い、かつ、当該申請に関して全責任を負う者。

４　手順

(1)　適合性証明のステップ

適合性証明を取得するためには、供給者適合宣言後、それを活用して登録適合性証明機関に申請者が適合性証明を依頼することにより登録適合性証明機関が一連の証明業務を行うことになる。適合性証明は強制されるものではないが推奨される。

(2)　供給者適合宣言

供給者適合宣言を行うためには、適合宣言書とその内容をトレースできる支援文書を準備しなければならない。

ア．適合宣言

適合宣言は JIS Q 17050-1 の規定に基づき行うこと。適合宣言書の様式は同規格の付属書 A を参考にすること。

イ．支援文書

適合宣言のためには支援文書の作成を要求されるが、その作成については JIS Q

17050-2 の規定によること。支援文書に必要な資料の例を次の a)～e)に示すが、必ずしもすべてが要求されるものではない。

a) 概要

宣言の対象となる製品及び／又はプロセスの説明とそれを特定できる型式、製造番号などの記述。

b) 機能安全管理

機能安全に取り組む体制が確立されているかを確認する（JIS C 0508 第 1 部第 6 項）

(b1) 安全方針
(b2) 関連する組織図
(b3) 品質マニュアル
(b4) 安全計画書
(b5) JIS C 0508 第 1 部への適合性を証明するチェックリスト

c) ハードウェア安全度

安全関連システムを構成する製品の安全度水準（SIL）の妥当性を確認する（JIS C 61508 第 2 部　7.4.4 項、7.4.5 項、付録 A 表 A.1 及び関連表、及び、付録 C）

（製品レベル）

(c1) 安全要求仕様書（リスクアセスメントシート含む）
(c2) 安全妥当性確認計画書
(c3) 回路図
(c4) FMEDA 計算書と使用データの出典
(c5) 安全マニュアル（ハードウェア及びソフトウェア）
(c6) 製品仕様書
(c7) 製品・システム全体を示す図面
(c8) 機能ブロック図（製品レベル）
(c9) 内蔵診断の説明
(c10) 製品コンポーネントの仕様表
(c11) 安全機能の定義
(c12) 製品のテスト結果
(c13) 使用証明の場合のフィールドデータ

（システムレベル）

(c14) 潜在危険リスク分析報告書
(c15) システムアーキテクチャ構成図
(c16) 機能ブロック図（システムレベル）

(c17) 信頼性ブロック図
(c18) SIL 計算書

d) 決定論的安全度（ハードウェア）

ハードウェアの決定論的原因故障に対する安全度を確認する（JIS C 0508 第 2 部 7.4.6　　、7.4.7 項、付録 A.3 の表 A.15、表 A.16、表 A.17、表 A.18、及び、、付録 B）

(d1) 製品仕様書
(d2) 製品テスト計画及びテスト結果
(d3) 製品の設計レビュー記録
(d4) 運転・保守マニュアル
(d5) JIS C 0508 第 2 部への適合性を証明するチェックリスト

e) ソフトウェア開発の審査

JIS C 01508 第 3 部への適合性を確認する。
(e1) ソフトウェア品質マニュアル
(e2) ソフトウェア安全計画書
(e3) ソフトウェア安全要求仕様書
(e4) ソフトウェア構成管理
(e5) ソフトウェア設計仕様書（アーキテクチャ、システム、モジュール）
(e6) ソフトウェア安全妥当性確認計画書及び報告書
(e7) ソフトウェア変更手順書
(e8) ソフトウェア変更の影響分析
(e9) 適合確認計画書、報告書
(e10) 安全マニュアル（ハードウェアに統合しても良い）
(e11) JIS C 0508 第 3 部への適合性を証明するチェックリスト
等

(3) 登録適合性証明機関による第三者証明

ア. 適合性証明申請

(ア) 適合性証明申請

適合性証明を取得しようとする申請者は、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）と本マニュアル 4.2 項に定め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。

（イ） 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、長期にわたることが多い。したがって、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。

(1) 新規開発の製品／システムの場合:　設計仕様がほぼ固まった段階、

(2) 既存の製品／システムの場合:　現行品の実力を知ること。必要に応じ設計変更を加える。設計変更の仕様がほぼ固まった段階。

イ.　適合性証明

登録適合証明機関は、申請を受けた場合は、次のように審査する。

（ア） 適合宣言の妥当性確認

登録適合証明機関は、4 項 (2) の適合宣言書と支援文書が 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を行う。

（イ） 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、4 項（2）の(b5)、(d5)、及び、(e11)　に基づく監査を行う。

（ウ） 証明

登録適合証明機関は、（ア）及び（イ）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できたら申請者に対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。

a)　証明書番号と発行日付
b)　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
c)　参照した規格リスト
d)　（必要であれば）付属書に使用される用語の定義
e)　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）
f)　外観
g)　安全状態
h)　証明された機能安全の範囲
i)　SIL 値、SIL 値を達成するための条件
j)　証明に使用した図面リスト
k)　システム要求に対する結果

l) 更新時、サーベイランス実施の要否

(4) 証明書の更新

ア. 有効期限

証明の有効期限は登録証明機関の定めによる。

イ. 更新手続き

(ア) 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。

(イ)有効期限内に規格改訂された場合

(ア)に準ずる。なお、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。

5.所轄労働基準監督署長による適合自動制御装置の認定

（1）登録適合性証明機関による適合性証明の対象となる範囲と審査内容

登録適合性証明機関による適合性証明は、制御システム全体として、要求安全度水準の適合性を証明する必要がある。コントローラ等の機器（デバイス）単位で要求安全水準の適合証明を受けている場合であっても、システムとして組み込んだ機械等の制限によってその安全度水準が達成できない場合があるためである。認定の対象となる適合自動制御装置には、新たに設置される機械等に備え付けられるもののみならず、すでに設置されている機械等を改修して新たに備え付けられるものも含まれる。

適合性証明にあたっては、リスクアセスメントにより、要求安全機能が適切に特定され、要求安全度水準が適切に設定されているかどうかが審査対象となる。同一型式による量産品に適合証明を行う場合、定期的に製造者に対するマネジメント監査も含まれる。

（2）要求安全度水準の決定のための使用条件の把握

要求安全度水準の決定には、ボイラーの設置場所等の機械等の使用条件に関する情報が必要であるため、機械等の使用者と製造者が連携し、使用条件を決定する必要がある。

ただし、大量に生産される同一型式のボイラーについては、あらかじめ機械等の使用条件を決定することは困難であるため、一定の使用条件を仮定してリスクを解析し、ボイラーの取扱説明書等により使用条件の制限やメンテナンス頻度の指定等を行う必要がある。

（3）所轄労働基準監督署長による、自動制御装置の使用条件及び用途・仕様と、被制御ボイラーの種類との整合性の確認

所轄労働基準監督署長は、認定を受けようとする適合自動制御装置に係る「用途及び仕様」及び「使用条件」が、それによって制御されるボイラーの「種類」「伝熱面積」等に合致していることを審査する。合致していなければ、自動制御装置が要求される機能を発揮できないためである。

このため、製造者が登録適合性証明機関に提出する「適合証明申請書」（登録省令様式第４号の３）や、登録適合性証明機関が発行する「適合証明書」（登録省令様式第４号の４）において、ボイラーの種類、自動制御装置の使用条件、用途・仕様が特定されている必要がある。

具体的には、適合証明申請書及び適合証明書の「使用条件」の欄には、当該自動制御装置の要求安全機能の特定及び要求安全度水準の決定の前提となっている、制御対象ボイラーの①種類（丸ボイラー（炉筒煙管ボイラー等）、水管ボイラー（貫流ボイラー等）、鋳鉄ボイラー又は特殊ボイラー（廃熱ボイラー等））、②燃料・熱源の種類（油、ガス、バイオマス、廃熱等）、③伝熱面積・内容積、④設置場所・条件、⑤自動制御装置の点検方法・頻度等を記載する必要がある。さらに、「用途及び型式」の欄には、証明対象の制御装置の用途に加え、当該機器が適合する安全度水準又はパフォーマンスレベルを記載する必要がある。

さらに、ボイラー設置者が所轄労働基準監督署長に提出する「適合自動制御ボイラー認定書申請書」（様式第 17 号）のボイラーの「種類」の欄には、適合自動制御装置に制御されるボイラーの種類及び燃料・熱源の種類を記載し、「伝熱面積又は内容積」の欄に、当該ボイラーの伝熱面積又は内容積を記載する必要がある。

参考文献

・ 「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の一部改正（指定外国検査機関関係を除く。）等について」（平成 28 年 9 月 30 日付け基発 0930 第 32 号）
URL:http://www.mhlw.go.jp/file/06-Seisakujouhou-11300000-Roudoukijunkyokuanzeneiseibu/0000140174.pdf

・ 「適合自動制御装置の認定実施要領」（平成 29 年 5 月 8 日付け基発 0508 第 2 号）
URL:http://www.mhlw.go.jp/file/06-Seisakujouhou-11300000-Roudoukijunkyokuanzeneiseibu/0000164326.pdf

様式第17号（第25条関係）

適合自動制御ボイラー認定申請書

事業場の名称		電話（　　）
事業場の所在地		
認定を受けようとするボイラー	製造許可番号及び許可年月日	
	検査証番号	
	種類	
	伝熱面積又は内容	
	検査証有効期間の末	
当該ボイラーに係る適合証明書の証明書番号及び証明年月日		

平成　　年　　月　　日

申請者氏名　　印

労働基準監督署長　殿

備考

1　ボイラーの設置場所を示す図面及び認定を受けようとするボイラーに係る適合　証明書(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様 式第４号の４）を添付すること。

2　氏名の記載及び押印に代えて、署名することができる。

様式第４号の３（第１条の２の 44 の６関係）

適合性証明申請書

1	製造者の名称	
2	製造者の住所	電話（　　）
3	品名及び型式	
4	適用した規格等	
5	用途及び仕様	
6	使用条件	

殿

年　　月　　日

申請者　　㊞

備考

1　本申請書には、ボイラー及び圧力容器安全規則第 25 条第２項に規定する厚生労働大臣の定める技術上の指針（以下「技術指針」という。）への適合性を明らかにする書面を添付すること。

2　適用した規格等の欄には、証明に当たって適用した技術指針以外の日本工業規格又は国際規格等の名称を記載すること。

3　用途及び仕様の欄には、証明対象機器の用途に加え、当該機器が適合する安全度水準（日本工業規格Ｃ0508）並びにカテゴリー及びパフォーマンスレベル（日本工業規格Ｂ9705）を記載すること。

4　氏名の記載及び押印に代えて、署名することができる。

様式第４号の４（第１条の２の 44 の６関係）

適合証明書

1	証明書番号		2	証明年月	年　　月
3	製 造 者 の 名				
4	製 造 者 の 住				電話（　　）
5	品 名 及 び 型				
6	適用した規格等				
7	用 途 及 び 仕				
8	使　　用　　条				
9	証明書の期限の末日				

年　　月　　日

殿

適合性証明機関

㊞

備考

1　適用した規格等の欄には､証明に当たって適用した技術指針以外の日本工業規格 又は国際規格等の名称を記載すること。

2　用途及び仕様の欄については､証明対象機器の用途に加え､当該機器が適合する 安全度水準日本工業規格Ｃ0508並びにカテゴリー及びパフォーマンスレベル（日 本工業規格Ｂ9705）を記載すること。

3　　氏名の記載及び押印に代えて、署名することができる。

第6章 演習事例

1. リスクアセスメントシート作成

(1) リスク分析、要求安全機能の特定

図 2-6　バーナ空気量不足の FTA 図例に基づき、空気量不足によるバーナ異常失火のリスク分析し、要求安全機能を特定しなさい。結果は、演習シート 1 の要求安全機能(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)の欄に記入すること。

なお、仕様、使用条件、保守点検、バーナ系統、燃焼制御系機能ブロック図は、下記の図表を条件とする。不足する情報があれば、各自で条件/仕様などを設定するか、その部分は空白として演習を進めてください。

表 1-2 ボイラーの仕様例
表 1-3 ボイラーの使用条件、保守点検
表 1-4 部品点検・交換リスト例
図 2-3 ガスバーナ制御系統の例
図 2-4 燃焼制御系機能ブロック図例

(2) 要求安全度水準の決定、使用者への情報

(1)で特定した要求安全機能の要求安全度水準、使用者への情報を決定しなさい。
結果は、(1)で作成した演習シート 1 に記入すること。
要求安全度水準の決定にあたって評価した各パラメータ(C,F,P,W)の評価理由を欄外に記載すること。
不足する情報があれば、各自で条件/仕様などを設定するか、その部分は空白として演習を進めてください。

2. SIL の評価

図 6-1 は、３．２．４ 低水位/燃焼系遮断の構成例（３）にエア圧スイッチ、エア圧スイッチ入力/RY1 リレー駆動部を追加したものである。
図 6-2 は、その追加したエア圧スイッチ入力/RY1 リレー駆動部の回路例である。

(1) 信頼性ブロック図

図 6-1 に基づき、エア圧スイッチ接点開により遮断弁で燃料を遮断する安全機能の信頼性ブロック図を作成しなさい。(演習シート 2-①)

(2) FMEDA 評価

FMEDA シートを使用して、図 6-2 エア圧スイッチ入力/RY1 リレー駆動部の FMEDA を実施しなさい。(演習シート 3)
●各部品のデータについて
故障率/故障モードのデータは、付録 1 を使用すること、その際にリレーコイルの故障率は 50(FIT)とすること。また診断率は付録 2 を使用し、リレー接点の監視が実施されている条件での診断率を使用すること。

(3) 構成要素の危険側故障率

(1)の信頼性ブロック図で示した各構成要素とその危険側故障率を表で示しなさい。
(演習シート 2-②)

なお、リレー接点の危険側故障率は 500(FIT)、エア圧スイッチの危険側故障率は 100(FIT)、遮断弁の危険側故障率は 5000(FIT)とする。

(4) 各構成要素(サブシステム)の PFDavg 算出

各構成要素(サブシステム)の PFDavg を計算し、各構成要素(サブシステム)の SIL(相当値)を示しなさい。(演習シート 2-③)

なお、プルーフテスト間隔などの条件は、1 項の演習内容を参考に設定して、その内容を明記すること。

(5) システムの SIL 値の結論

PFDavg の合計からシステムの SIL 値を算出し、アーキテクチャ制約からの SIL 値を確認し、システムの SIL 値の結論を示しなさい。(演習シート 2-④,⑤,⑥)

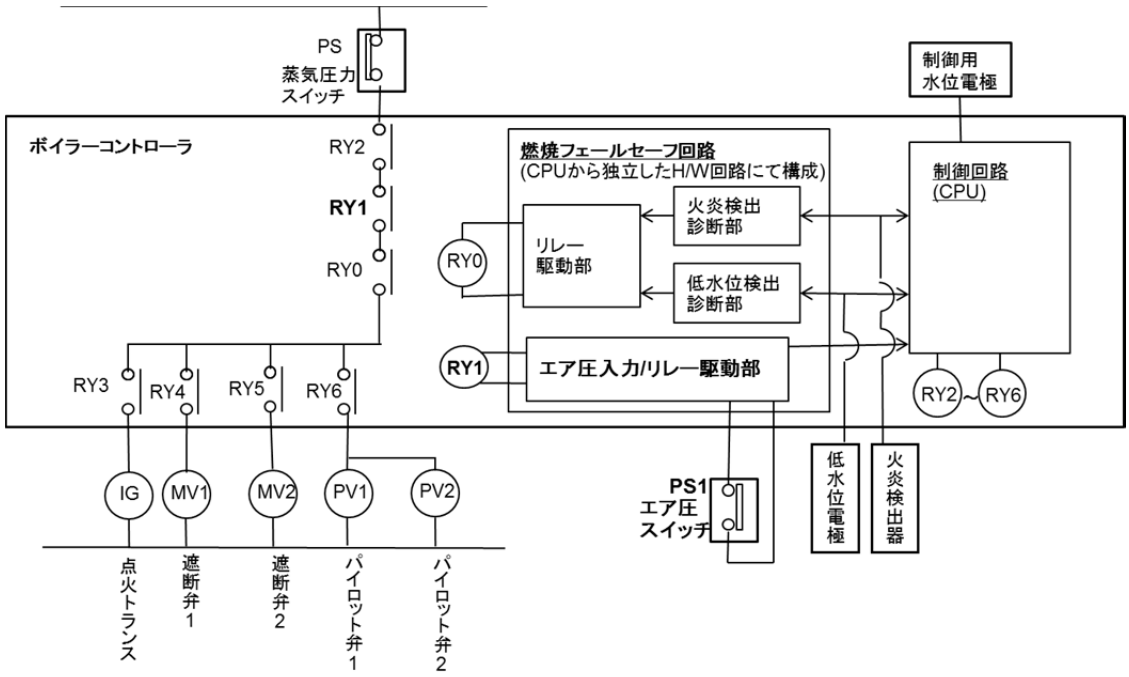


図 6-1　演習-構成例

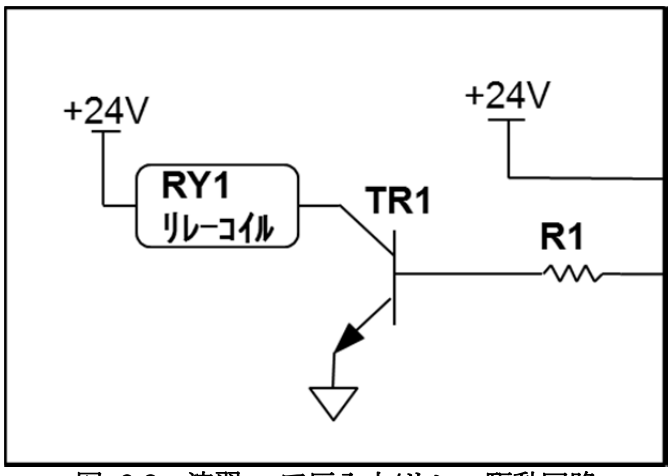


図 6-2　演習-エア圧入力/リレー駆動回路

【演習シート１】

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
各パラメータ(C,F,P,W)の評価理由													

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

【演習シート 2】

①信頼性ブロック図

②構成要素の危険側故障率

記号	構成要素	危険側故障率 λD(FIT)

③サブシステムの計算条件と結果

項目				
構成(1oo1、1oo2、、)				
PFDavg の計算式(63 ページ参照)				
危険側故障率 λD(FIT)				
DC				
検知不可危険側故障率(FIT)				
検知可能危険側故障率(FIT)				
プルーフテスト間隔 T1(年)				
平均修理時間 MRT(時間)				
平均修復時間 MTTR(時間)				
tCE(時間)				
tGE(時間)				
βD(%)				
β(%)				
PFDavg				
SIL				

プルーフテスト間隔の設定に対する説明：

④ランダムハードウエア故障確率　PFDavg 合計からの SIL 値

⑤アーキテクチュアの制約からの SIL 値

⑥システムの SIL 値の結論

演習シート 3（FMEDA 評価シート）

番号	部品名称	全故障率(FIT)	故障モード	分配率(%)	故障率(FIT)	安全側/危険側	診断率(%)	λ_{SD}(FIT)	λ_{SU}(FIT)	λ_{DD}(FIT)	λ_{DU}(FIT)	$\lambda_{\text{No Effect Failure}}$(FIT)	$\lambda_{\text{No Part Failure}}$(FIT)

付録１　故障率・故障モード（EN 13611:2007）

EN 13611:2007 の故障率データを示す。この故障率は SN 29500 をもとにして雰囲気温度 60℃、ディレーティングが 67%の場合において評価している。また、周囲条件及び(又は)負荷条件が規定値と異なる場合、故障率が再計算されなければならない。
表 J.3 に含まれるもの以外のコンポーネントの個々の故障率はメーカーによって提供される故障率を使用して決定されなければならない。これは、特にリレー、火炎検出部などに適用することがある。
B10d 値を使用したリレーの故障率を決定する方法は、J.5.4.4.3 の中で与えられる。

注 1　簡単に計算するため、故障率は故障モードの数を考えて同じ割合で分割される。
例えば、ダイオード用の基礎故障率 λ B は、フォールト・モード「オープン」と「ショート」に分割されて、λ open = λ short = λ B/2 となる。
注 2　表 J.3 で与えられる故障率と周囲及び負荷条件を計算する方法は、SN 29500 シリーズのデータベースから得られた。

故障率・故障モードの使用にあたっては、規格の他の注意事項も参照すること。

表 J.3 故障率と故障モード

コンポーネントタイプ	故障モード							故障率	
	ショート	オープン	ドリフト 1/2x	ドリフト 2x	その他	ピン数	フォールト数	コンポーネント故障率 λ (FIT) a	フォールトあたりの故障率 λ (FIT)
列	1	2	2a	2b	2c	3	4	5	6
抵抗									
カーボンフィルム		1				2	1	1.6	1.6
金属フィルム		1				2	1	0.3	0.3
金属酸化膜		1				2	1	8.0	8.0
巻き線型	1	1				2	2	8.0	4.0
抵抗体素子のネットワーク	1	1				2	2	0.2	0.1
可変抵抗器									
巻き線型(一層)		1				3	3	48.0	16.0
その他	1	1				3	6	48.0	8.0
バリスタ	1	1				2	2	1.0	0.5
PTC サーミスタ	1	1	1	1		2	4	5.0	1.25
NTC サーミスタ	1	1	1	1		2	4	3.0	0.75
コンデンサ									
EN 60384-16 に従う金属化フィルム:MKT、MKP、MKU		1				2	1	4.3	4.3

コンポーネントタイプ	故障モード							故障率	
	ショート	オープン	ドリフト 1/2x	ドリフト 2x	その他	ピン数	フォールト数	コンポーネント故障率 λ (FIT) a	フォールトあたりの故障率 λ (FIT)
列	1	2	2a	2b	2c	3	4	5	6
EN 60384-16 に従う金属化フィルム:MKC		1				2	1	7.3	7.3
金属箔:KC		1				2	1	20.9	20.9
金属箔:KS、KP、KT		1				2	1	7.4	7.4
金属化紙(フィルム):MP、MKV)	1	1				2	2	12.4	6.2
セラミック:NDK/ LDC, COG, NPO	1	1				2	2	4.8	2.4
セラミック:HDK/MDC、X7R、X5R	1	1				2	2	9.7	4.8
セラミック:HDK/HDC、Z5U、Y5V、Y4T	1	1				2	2	24.2	12.1
アルミニウム電解質(固体電解質)	1	1	1			2	3	2.2	0.75
タンタル電解質(固体電解質)	1	1	1			2	3	51.8	17.3
可変	1	1				2	2	14.0	7.0
インダクタ、変圧器									
LF インダクタ、変圧器	1	1				2	2	7.0	3.5
emc 抑制用インダクタ	1	1				2	2	2.1	1.05
スイッチモード電源の主変圧器および変圧器[b]	1	1			-4	4	6	48.0	8.0
スイッチモード電源の主変圧器および変圧器	1	1				4	10	48.0	4.8
ダイオード等									
ユニバーサル、ショットキーダイオード	1	1				2	2	2.3	1.15
サプレッサーダイオード	1	1				2	2	16.8	8.4
Z ダイオード<1W	1	1				2	2	2.4	1.2
Z ダイオード>1W	1	1				2	2	47.5	23.8
定電圧ダイオード	1	1	1	1		2	4	16.1	4.0
整流ダイオード	1	1				2	2	4.0	2.0
整流器ブリッジ	1	1				4	10	20.0	2.0
ディアック[c]	1	1			2	2	4	150.0	37.5
トランジスタ等									
バイポーラ、ユニバーサル、例えば TO18、TO92、SOT23	1	1				3	6	7.6	1.3

コンポーネントタイプ	故障モード							故障率	
	ショート	オープン	ドリフト 1/2x	ドリフト 2x	その他	ピン数	フォールト数	コンポーネント故障率 λ (FIT) a	フォールトあたりの故障率 λ (FIT)
列	1	2	2a	2b	2c	3	4	5	6
バイポーラ低消費電力、例えば TO 5、TO39	1	1				3	6	52.8	8.8
トランジスターのトランジスターアレイ	1	1				3	6	38.0	6.3
バイポーラパワー、例えば TO3、TO220	1	1				3	6	132.0	22.0
FET 接合、MOS	1	1				3	6	12.7	2.1
MOS、パワー、例　TO3、TO220	1	1				3	6	264.0	44.0
サイリスタ[c]	1	1			2	3	8	100.0	12.5
トライアック[c]	1	1			2	3	8	150.0	18.5
集積回路[d e]									
μC/ASIC/PLD≦32pin[CORE]								50.0	
[IC]	1	1				16	57	194.2	3.41
μC/ASIC/PLD＞32pin[CORE]								100.0	
[IC]	1	1				40	153	487.1	3.18
EEPROM	1	1				28	105	310.0	2.95
OpAmp バイポーラ	1	1				8	25	13.8	0.55
OpAmpCMOS、基準要素	1	1				8	25	8.8	0.35
コントローラ（スイッチングレギュレータ）	1	1				6	17	23.0	1.35
トランズミッタ/レシーバ/ADC	1	1				8	25	23.0	0.9
CMOS/TTL 論理ゲート	1	1				16	57	11.5	0.2
光電子コンポーネント									
フォトカップラー、バイポーラ出力	1	1				4	10	42.0	4.2

コンポーネントタイプ	故障モード							故障率	
	ショート	オープン	ドリフト 1/2x	ドリフト 2x	その他	ピン数	フォールト数	コンポーネント故障率 λ (FIT) a	フォールトあたりの故障率 λ (FIT)
列	1	2	2a	2b	2c	3	4	5	6
フォトカップラー、FET 出力	1	1				4	10	104.0	10.4
Si フォトダイオード/Si PIN フォトダイオード	1	1				2	2	5.7	2.9
Ge フォトダイオード	1	1				2	2	185.0	92.5
Si フォトトランジスタ	1	1				3	6	6.3	1.05
フォトエレメント	1	1				2	2	6.0	3.0
フレームセンサー（光レジスター等）[f]	1	1				2	2		
UV 管	1	1				2	2	50000	25000
リレー[g]									
コイル	1	1				2	2		
接点	1	1				2	2		
クリスタル、水晶発振子[h]	1	1				2	2	15.0	7.5
セラミック共振子[h]	1	1				2	2	5.0	2.5
ヒューズ		1				2	1	25.0	25.0
避雷器（ガス充てん）	1	1				2	2	1.0	0.5
スイッチ									
DIP スイッチ、接点あたり	1	1				2	2	0.3	0.15
パワースイッチ、接点あたり	1	1				2	2	80.0	40.0
ジャンパー		1				2	1	1.0	1.0
ケーブル		1				2	1	1.0	1.0

注　列の説明:
1;2　EN 13611 からの故障モード
2a、2b　故障モード「公称値の半分のドリフト」、「公称値の 2 倍までのドリフト」、
2c　特別な故障モード(脚注を参照)
3　コンポーネントあたりの接続ピンの数
4　1、2、2a、2b、2c 及び 3 に起因するフォールト数
5　コンポーネントあたりの故障率(脚注 a を参照)
6　フォールトあたりの故障率

コンポーネントタイプ	故障モード							故障率	
	ショート	オープン	ドリフト 1/2x	ドリフト 2x	その他	ピン数	フォールト数	コンポーネント故障率 λ (FIT) a	フォールトあたりの故障率 λ (FIT)
列	1	2	2a	2b	2c	3	4	5	6

a 故障率は、基礎故障率、EN 13611 の最大周囲温度条件(+60℃)に基く温度依存ファクター π_T、$U/U_{max} = 0.7$(EN 61508-2:2010,7.4.2.13 による 67%のディレーティング)で計算された電圧依存ファクター π_U 及び負荷依存ファクター π_L に対して計算される。

b 故障モード排除「短絡回路 1 次/2 次」("-4 は次を意味する:フォールト総数は排除された短絡の数によって減少する」)。

c 2c 列の故障モード「半波モード A/K」、「半波モード K/A」。

d 3 列にピン数の入力(n =ピンの数)。

e 故障率$_{[IC]}$=故障率$_{[CORE]}$+(n *故障率$_{[バイポーラトランジスター]}$/3) →4 列

$N_{[IC]}$＝故障モード数= $N_{[短絡]}$＋$N_{[断線]}$

$N_{[短絡]}$=(n-1)+(n - 2)+(n - 4);

隣接ピンの短絡、およびピンと+V_{CC} 間の短絡及びピンと V_{CC}(GND)間の短絡。

$N_{[断線]}$= n

f 個々に決定されること;J.5.4.4.2 を参照

g 故障率は個々のコンポーネントに対して決定されなければならない;J.5.4.4.3 を参照。故障率は各接点に適用される。

h 低調波/高調波は、EN 13611 によってカバーされる。

付録２　診断率（EN 13611:2007）

表 J.1 と表 J.2 は関連する診断率（DC)のレベルを達成するランダムハードウェア故障を検知・制御する診断テストの技術と方策を提供する。
診断テストが下表の「参照」の要求事項に適合する場合に、その診断率(DC)を計算に使用してもよい。他の方策および技術は、主張された診断率を支援する証拠がある場合に使用できる。

表 J.1- 診断技術

診断技術	参照	DC	備考
オン・ライン監視による故障検出	EN 61508-2:2010、A.2、A.3	90 %	故障検出の診断率に依存する。
アイドル電流原理	EN 61508-2:2010, A.2, A.15	60 %	電気機械システム、アクチュエータ
リレー接点の監視	EN 61508-2:2010、A.2、A.15	99%	電気機械システム、アクチュエータ
コンパレータ	EN 61508-2:2010、A.2、A.3	99%	主として故障モードが安全側にある場合、高
多数決投票	EN 61508-2:2010、A.2、A.3	99%	投票の質に依存する。
冗長ハードウェアによるテスト	EN 61508-2:2010、A.3	90%	故障検出の診断率に依存する。
動的な原理	EN 61508-2:2010、A.3	90%	故障検出の診断率に依存する。
監視冗長	EN 61508-2:2010、A.3	90%	故障検出の診断率に依存する。
タイムウィンドウのない分離したタイムベースのあるウォッチドッグ	EN 61508-2:2010、A.10、A.12	60%	プログラムシーケンス、クロック
タイムウィンドウのある分離したタイムベースのあるウォッチドッグ	EN 61508-2:2010, A.10, A.12	90%	プログラムシーケンス、クロック
プログラムシーケンスの一時的・論理的な監視の組合せ	EN 61508-2:2010、A.10、A.12	99%	プログラムシーケンス、クロック
安全シャット・オフのある過電圧保護	EN 61508-2:2010、A.9	60%	電源
安全シャット・オフのある二次電圧制御および防護	EN 61508-2:2010、A.9	99%	電源

表 J.2 診断方策

診断方策	参照	DC	備考
テストパターン	EN 61508-2:2010, A.7	99 %	I/O 装置
アナログ信号監視	EN 61508-2:2010, A.3, A.14	60 %	I/O 装置、センサー
リファランスセンサー	EN 61508-2:2010, A.14	90 %	センサー
修正チェックサム	EN 61508-2:2010, A.5	60 %	不変メモリ(ROM)
シングルワード（8 ビット）の署名（CRC）	EN 61508-2:2010, A.5	90 %	不変メモリ(ROM) 署名の有効性は、保護される情報のブロック長に関係する署名の幅に依存する。
ダブルワード（16 ビット）の署名（CRC）	EN 61508-2:2010, A.5	99 %	不変メモリ(ROM) 署名の有効性は、保護される情報のブロック長に関係する署名の幅に依存する。
RAM テスト「チェッカーボード」又は「マーチ」	EN 61508-2:2010, A.6	60 %	可変メモリ(RAM)
RAM テスト「ウォークパス」	EN 61508-2:2010, A.6	90 %	可変メモリ(RAM)
RAM テスト「ガルパット」又は「透明ガルパット」又は「アブラハム」	EN 61508-2:2010, A.6	99 %	可変メモリ(RAM)
ハードウェア又はソフトウェア比較、および読み書きテストのあるダブル RAM	EN 61508-2:2010, A.6	99 %	可変メモリ(RAM)
ソフトウェアによるシングルチャンネルの自己テスト（ウォーキングビット）	EN 61508-2:2010, A.4	90 %	演算処理装置(CPU)
ソフトウェアによる相互の比較	EN 61508-2:2010, A.4	99 %	演算処理装置(CPU);比較の質に依存する。
情報の冗長	EN 61508-2:2010, A.8	99 %	内部通信

付録３　共通原因故障モデル（EN 13611:2007）

ここで述べる手法は、EN 61508-6, 2010 付属書 D を修正したものである。
複雑なシステムの場合で表 J.4 のいずれの項目もあてはまらない場合は、β = 2%の共通原因ファクターを使用しなければならないとしている。また。表 J.4 の項目の少なくとも 1 つがあてはまる場合は、J.4 を使用して X 及び Y を集計して β を決定するとしている。

表 J.4 — 電子又はセンサー/アクチュエータのスコア

項目	電子制御		センサー/アクチュエータ	
	X	Y	X	Y
冗長チャネルが検出部に異なる電気的技術(例えば、一方がプログラマブル、他方がリレー)、アクチュエータに異なる物理的な原理を使用する。	7		7.5	
冗長チャネルがセンサーに異なる電子技術(例えば、一方が電子、他方がプログラマブル電子)、又は異なる電気的な原理/設計(例えばディジタル、アナログ)、アクチュエータ(例えば異なるメーカー又は技術)を採用する。	5		5.5	
多様性中、例えば異なる技術を使用するハードウェア診断テストの使用	3	1.5		
チャネル間の交差結線は、診断テスト又は投票目的に使用された以外の情報の交換を妨げる。	0.5	0.5	0.5	0.5
同じハードウェアで同様の環境の中で5年以上の使用経験がある。	1.0	1.5	1.5	1.5
すべてのフィールド故障が、設計に充分にフィードバックされて分析析されているか。(手順の証拠書類が必要である。)	0.5	3.5	0.5	3.5
全てのコンポーネント故障(又は劣化)が検知されること、根本的原因が確証されたこと、及び同様なアイテムが故障の同様の潜在的な原因について調査されたことを保証する作業の書面によるシステムがあるか?		1.5	0.5	1.5
システムは診断率中(> 90%…<99 %)を有している。	1.5	1.0		
システムには診断率高(> 99 %)である。	2.5	1.5		
設計者は、共通原因故障の原因及び結果を理解するように(教育資料で)訓練されたか。	2.0	3.0	2.0	3.0
システムは外部環境を制御することなく常に温度、湿度、腐食、ダスト、振動などの範囲(テストされた範囲)内で動作するか。	3.0	1.0	3.0	1.0

表 J.5 から β の値を得るためにスコア値 S =X+Y+40 を計算する(注を参照)。

表 J.5 — β の計算

スコア (S)	β	
	電子制御	センサー/アクチュエータ
100 or above	0,5 %	1 %
60 to 100	1 %	2 %
40 to 60	2 %	5 %

注 1、EN 61508-6:2010 表 D.1 の次の側面が EN 13611 や適用可能な製品規格において原理的に適用可能であり、Xmin = 17 および Ymin = 23(Smin = Xmin+Ymin = 40)が与えられる:

**多様性低(例えば同じ技術を持ったハードウェア診断テスト)の使用。
**機器で使用された技術に基づいた設計は、>5 年間、フィールドで成功裡に使用されている。
**簡単なシステム(低 I/O 複雑さ)。
**過電圧/過電流に対して保護された I/O(義務としての emc、及び電気的強度試験による妥当性確認)。

**共通原因故障の源が FMEA によって検知され、設計によって除去される。
**共通原因故障が設計レビューで検討され、結果が設計にフィード・バックされる。
**システムには少なくとも低い診断率(> 60%…<90%）がある。
**ユーザアクセスが技術的及び、または組織的な方策によって制限される。
**信号及び供給配線が十分に分離される。(義務的な em、及び電気的な強度試験による妥当性確認)
**システムが安全面を考慮した包括的な環境試験の主題である。

注 2 それらの測面は、全体像を良く示すために表 J.4 から除外された。