

機能安全が可能にする機械の安全確保

－ ボイラー編 －



厚生労働省では、「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）を発行し、機能安全を活用した機械等の安全確保を推進しています。

ボイラーにおいては、平成 28 年 9 月に、機能安全による安全確保を労働安全衛生法令に位置づけ、安全規制の高度化を図るため、関係法令の改正が行われました。

このパンフレットは、ボイラーへの機能安全の導入について、ご理解いただきたい概要をまとめたものです。

平成 28 年度厚生労働省委託

中央労働災害防止協会

機能安全の導入による安全規制の高度化

●背景

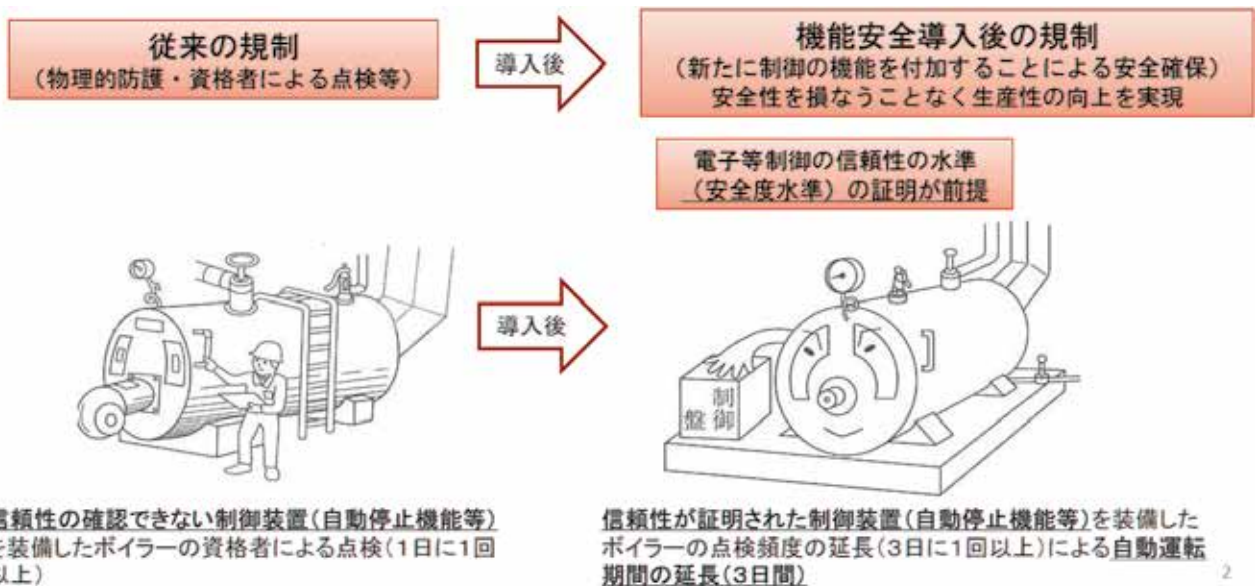
- ▶ 近年、電気・電子技術やコンピュータ技術の進歩に伴い、これら技術を活用することにより、機械等に対して高度かつ信頼性の高い制御が可能となってきています。
- ▶ 機能安全について国際規格が定められ、欧米では、機能安全を導入した高い信頼性を持つ自動制御装置を装備した機械等に対して、機械等の取扱規制を見直す動きがあります

●基本的な考え方（機能安全指針）

- ▶ 従来の機械式の安全装置等に加え、新たに電子等制御の機能を付加することにより、機械等によるリスクを低減するための措置（機能安全）による安全確保を推進します（「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。）

●ボイラーでは

- ▶ ボイラーにおいては、平成28年9月に、機能安全による安全確保を労働安全衛生法令に位置づけ、安全規制の高度化を図るため、関係法令の改正が行われました。



ボイラーの取扱規制の改正

●ボイラー及び圧力容器安全規則の改正

ボイラーは、容器の厚さや安全弁といった物理的防護に加え、ボイラー及び圧力容器安全規則（以下「ボイラー則」という。）第25条により、ボイラー技士による常時監視や、水面測定装置の機能の1日1回の点検を義務付けています。従来、異常があった場合に自動的にボイラーを停止する「自動停止機能」は設けられていましたが、その信頼性についての定めは特になく、最後

の砦として、ボイラー技士が常時監視し、異常があった場合には、ボイラーを停止させることを前提としていました。

機能安全を導入すれば、自動制御の信頼性である「安全度水準 (SIL/Safety Integrity Level)」により、いざというときに自動制御が故障する確率が非常に低いことが定量的に明らかになります。このため、そのような証明がされた自動制御装置を装備したボイラーについては、ボイラー技士による常時監視を外すとともに、水面測定装置の機能の点検の頻度を3日に1回とすることが妥当であるとされました。これにより、ボイラー技士の負担軽減と生産性の向上を図ることが可能となります。平成 28 年 9 月にボイラー則等は改正され、平成 29 年 4 月 1 日から施行される予定です。

ボイラー則に規定する事項

- 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厚生労働大臣の定める技術上の指針に適合していることを所轄労働基準監督署長が認めたものを備えたボイラーについては、水面測定装置の機能の点検の頻度を、1日に1回以上必要であるところ、3日に1回以上(※)とすることができる。
※ 欧州規格等においては、機能安全を採用しているボイラーに係る検査間隔を72時間以下とすることを定めている。
- 1の所轄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に、当該申請に係る自動制御装置が1の厚生労働大臣が定める技術上の指針に適合していることを厚生労働大臣の登録を受けた者が証明した書面を添付して所轄労働基準監督署長に提出しなければならない。

●遠隔制御監視基準の改正

ボイラーの遠隔制御監視基準等についての通達も改正され、従来の方法(別添1、別添2)に加えて、別添3が追加となり、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りました。

| ボイラーの遠隔制御監視基準等について (基発 0331001 号) | |
|---|--|
| 従来の基準 | 別添 1 : 遠隔監視室で監視するボイラー <ul style="list-style-type: none"> 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 |
| | 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 <ul style="list-style-type: none"> 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 |
| 平成28年9月 基発0930第35号 機能安全導入により追加された基準 | 別添 3 : 認定適合自動制御装置を備えたボイラー <ul style="list-style-type: none"> 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 |

●ボイラー取扱作業主任者の選任基準の改正

さらに、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 号の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）も伝熱面積に参入しないボイラーとすることが可能となりました。

| | |
|--|--|
| 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）で定めた自動制御装置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） |
| これに機能安全を追加するより安全基準追加入 | 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) |

●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係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」が新設されました。労働基準監督署長の認定を受けようとする事業者は、「登録適合性証明機関」が証明した適合証明書及び下記の付属書面を添付して所轄労働基準監督署長に申請します。

1. 証明書番号と発行日付
2. 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
3. 参照した規格リスト
4. (必要であれば) 付属書に使用される用語の定義
5. 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)
6. 外観
7. 安全状態
8. 証明された機能安全の範囲
9. SIL 値、SIL 値を達成するための条件
10. 証明に使用した図面リスト
11. システム要求に対する結果
12. 更新時、サーベイランス実施の要否

機能安全指針に基づく安全関連システムの設計

厚生労働省で定めた機能安全指針では、「機能安全に係る実施事項」として、次の①から③の3ステップが定められています。

①要求安全機能の特定

①-1 危険性又は有害性及び危険事象の特定

はじめに、リスクを解析することにより、労働者の就業に係る危険性又は有害性を特定し、その結果として発生する危険事象を特定します。

①-2 要求安全機能の特定

特定された危険事象を防止するために必要となる要求安全機能を特定します。
(要求安全機能とは、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)

①-3 安全関連システムの特定

特定した要求安全機能を実現するために必要な安全関連システムを特定します。この安全関連システムは、検出部(センサー)等の入力部、論理処理部及びアクチュエータ等の出力部が含まれるものであり、ボイラーを運転制御するシステムから独立していることが望ましいとされています。

②要求安全度水準(SIL)の決定

要求安全度水準とは、特定した安全関連システムに要求される信頼性の水準であり、国際安全規格 IEC61508/JISC0508 の基準又はこれと同等以上の基準に適合することが必要です。要求安全度水準は、労働者が危険性又は有害性にさらされる頻度、生ずる負傷又は疾病の重篤度、危険事象を回避する可能性、要求安全機能の作動が求められる頻度等を用いた定性的評価によって決定します。

③設計要求事項の決定とそれに基づく製造

要求安全度水準のレベルに応じて、作動失敗の確率の基準を満たすことができるように、制御装置を設計し、製造します。

安全度水準は、危険事象に至る安全関連システムの故障(危険側故障)の確率で表され、危険側故障確率、検査間隔、平均修理時間、共通原因故障によって計算されます。

製造者は、安全関連システムの多重化による共通原因故障の低減、自動的な診断等による検知できない危険側故障に係る確率の低減、検査間隔の短縮等を安全関連システムに設計上求められる事項として定め、これらに基づいて製造します。

ボイラーの安全関連システムの設計例

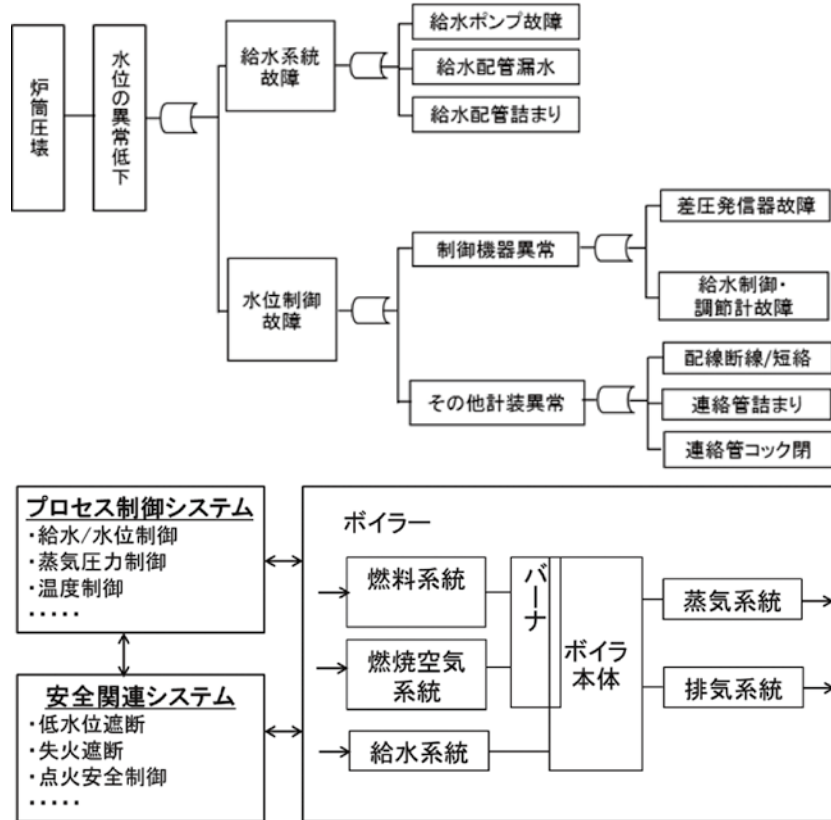
機能安全指針に基づく、ボイラーの安全関連システムの設計の手順の一例を以下に示します。

①要求安全機能の特定

①-1 危険性又は有害性及び危険事象の特定

●リスクアセスメント範囲の指定

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します。



●ボイラーの仕様及び使用条件

ボイラー種類、型式、一般仕様・容量、制御方式などを仕様として定義し、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/設置環境、保守・点検の内容とその周期などを決定します。

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) |

●リスク分析

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します。

炉筒煙管ボイラーの FTA 例 (水位の異常低下)

①-2 要求安全機能の特定～②要求安全度水準の決定

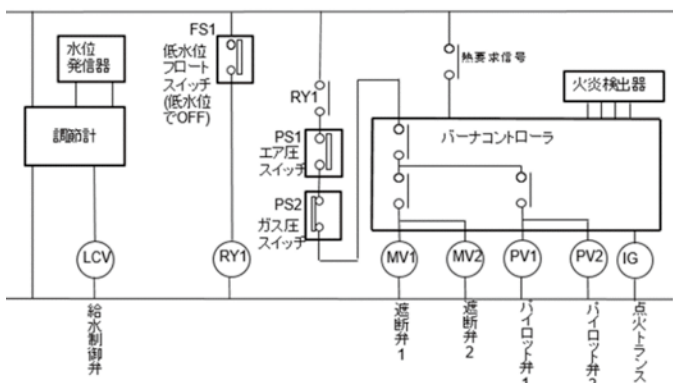
FTA などで実施したリスク解析の結果に基づき、下表のように要求安全機能ごとの要求安全度水準、使用者への情報を決定します。

| 要求安全機能の特定 | | | | | | | 安全度水準決定 (SIL) | | | | | 使用者への情報 | |
|-----------|--------|---------------|--------------------|--------|----------------------------------|--------------------------------------|----------------|----------------|----------------|----------------|-----|----------|------------------------|
| 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 / 空炊きによる火災または圧壊 | 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 | 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 | 給水系統の配管、機器の漏れの日常点検 |

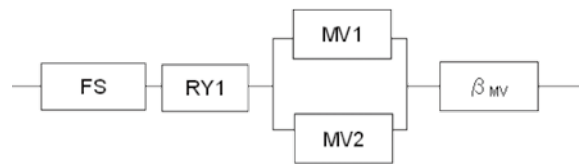
③設計要求事項の決定とそれに基づく製造

●機能ブロック図、信頼性ブロック図

機能ブロック図を作成し、それをもとにして要求安全機能ごとに信頼性ブロック図を作成します。



機能ブロック図 (低水位 / 燃焼系遮断の例)

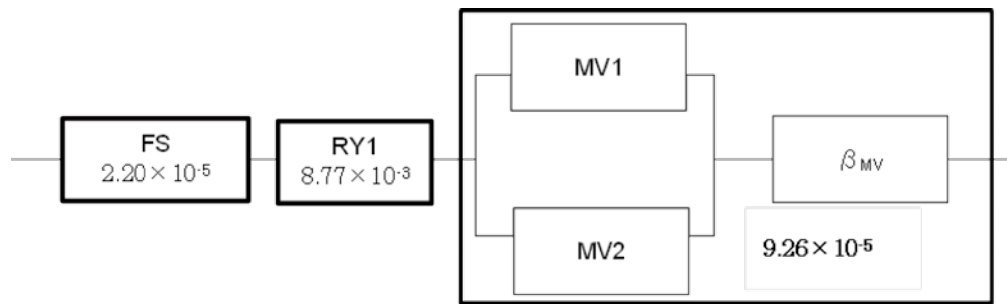


FS : 低水位スイッチ、RY1 : リレー、MV : 遮断弁
β_{MV} : 遮断弁 1、2 の共通原因故障

信頼性ブロック図 (低水位遮断の例)

●平均危険側失敗確率 (PFDavg) の計算と安全度水準の評価

信頼性ブロック図の各構成要素の危険側故障率、プルーフテスト間隔 (検査間隔)、平均修理時間、共通原因故障から、平均危険側失敗確率 (PFDavg) を計算します。



$$PFD_{avg} = 2.20 \times 10^{-5} + 8.77 \times 10^{-3} + 9.26 \times 10^{-5} = 8.89 \times 10^{-3}$$

となり、この PFD_{avg} は、安全度水準SIL2に該当します。

(安全度水準を確定するには、アーキテクチャ制約の要求からも評価が必要になります)

以上により、①-2の表で示した要求安全機能(低水位遮断)と要求安全度水準(SIL2)が、本例の構成で達成されたこととなります。

機能安全活用テキストと実践マニュアル

本パンフレットとともに作成した「機能安全活用テキスト」、「機能安全活用実践マニュアルーボイラー編ー」では、ボイラーの安全関連システムへ機能安全を導入する上で必要となる機能安全の考え方や、設計手順が解説されています。機能安全について学習する場合はテキストを、ボイラーの安全関連システムの設計手順について学習する場合はマニュアルをご覧ください。主な項目は次の通りです。(これら図書はおって厚生労働省ウェブサイトに掲載される予定です。)

「機能安全活用テキスト」

- 機械設備の安全概論
- 法令と規格体系
- リスクアセスメントとリスク低減
- 機械安全における機能安全の適用
- 機能安全による安全関連制御システムの設計
- 妥当性確認

「機能安全活用実践マニュアルーボイラー編ー」

- ボイラーのリスクアセスメント(機械類の制限の決定)
- 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ほか
- 要求安全度水準に適合する設計(システム設計)
- 妥当性確認
- 第三者認証
- 付録