A1607-15
0385-9886/16/¥500/論文/JCOPY

《特集：機能安全の現状と動向》

機械設備における機能安全の役割と取扱規制に対する厚労省の取り組み

The role of functional safety in machinery and equipment and the efforts of the Ministry of health for handling regulations

明治大学　向殿　政男

はじめに

“機能安全”という言葉が多くの安全の分野、特に安全制御の世界で盛んに聞かれるようになってきた。労働安全や機械安全でも例外ではない。本稿では、そもそも機能安全とはどのような考え方であるのかという基本的なことについて、かなり詳しく解説をした後、機能安全の使い方を簡単に紹介をする。現在、厚生労働省では、労働安全衛生法令の中で機能安全を取扱規制として、どのように適用できるかの検討に入った。このことについての厚労省の取り組みの動向について簡単に紹介をする。

1. 機能安全という考え方について

機能安全（Functional Safety）とは、「正しく機能することにより実現される安全機能（Safety Function）」のことであるというのが機能安全の単純な用語の意味である。しかし、現実に用いられている機能安全はもう少し狭い意味になっている。これを現実に即して正しく理解するためには、まず、安全機能（Safety Function）とは何かを知らなければならない。

安全機能とは、簡単に言えば、安全を確保する機能のことである。通常、対象としているシステムは、二つの機能を持っている。一つは、そのシステムの本来のミッションとして遂行すべき本来機能（例えば、ものを運ぶとか、ものを削るとか等の機能）であり、もう一つは、それを安全に達成するために必要な機能である。この後者が安全機能である。ちなみに、機械安全における制御安全の国際規格[1]では、安全機能とは、「故障がリスクの増加に直ちにつながるような機械の機能」と定義されている。

更に、安全機能にも二つのタイプがあることに気が付かなければならない。一つは、対象としているシステム本体自身が持っている安全機能である。例えば、構造計算に基づき頑強に作って安全を確保するとか、サブシステムが故障すると安全側になるようにフェールセーフに設計するとか、人間が間違えると動かないようにフールプルーフに設計するとかのような構造による安全機能、更には、故障しないように高信頼の部品を使用したり、冗長系に基づく高信頼化技術等による信頼度に基づく安全機能等は、システム本体に組み込まれている安全機能である。これらは、本質的安全による安全機能といわれている（筆者は、本質的安全の中でも、危険源の除去も含めて前半の構造によるものを本質安全と呼び、本質的安全とは区別している：的という用語が入るか入らないかの違いである）。もう一つのタイプの安全機能は、付加的に取り付けられた装置により実現される安全機能である。例えば、安全柵や安全センサー等の安全装置などが実現する安全機能である。現在の機能安全という用語は、安全確保のために付加的につけられた装置が実現する後者の安全機能のために用いられている。従って、冒頭の機能安全の解説は、「システムの安全のために付け加えられたサブシステムが、正しく機能することにより、システム全体の安全を確保する機能」

のことであるといえば、もう少し詳しくになるだろう。

機能安全を更に詳しく理解するためには、更なる二つの考え方のペアを知らなければならない。一つは、システムを安全関連系と非安全関連系に分けるという考え方である。もうひとつは、制御されるもの（EUC：Equipments Under Control：被制御系）と、制御するもの（EUCを制御する系）とに分類するという考え方である。安全関連系とは、安全機能をつかさどっているサブシステムであり、安全装置はその典型例である。非安全関連系とは、システムの本来の機能等を実現している部分で安全機能には関連していないサブシステムのことである。機能安全は、もちろん安全関連系が果たしている機能のことである。前述したように、安全関連系にはシステム本体に内在するものと外部から付加的に付け加えたものとがあることに注意する必要がある。また、最近のシステムは、電気や電子やコンピュータでの制御を利用しているものが多く、その場合には、制御されているサブシステム（EUC被制御系）とそれを制御しているサブシステム（EUC制御系）と区別して考察する必要がある。機能安全は、EUC制御系が果たす安全機能を対象としている。EUC制御系にも本来の機能のための制御系と、安全機能を実現するために付加的に付け加えられている制御系とがあることに注意する必要がある。本稿の主題の機能安全は、以上のように、主として、安全関連系に対して、また、EUC制御系に対して注目をしており、それらが正しく機能することで実現される安全機能を問題にしている。ここまでくると、機能安全のもう少し現実的な定義は、「システムの安全のために、付加的に導入された制御系の機能が正常であることによって達成される安全」となるだろう。

これまでの機械安全の世界では、最後の最後は伝統的に機械式の安全装置で安全が確保されてきた。最近、機能安全が注目をされるようになったのは、コンピュータ等のソフトウエアを含んだ高度な電気、電子装置が安全機能を司るようになってきたからである。機能安全の規格である国際安全規格IEC 61508（JIS C 0508）[2]では、機能安全を「EUC及びEUC制御系の全体に関する安全のうち、E/E/PE 安全関連系及び他リスク軽減措置の正常な機能に依存する部分」と定義している。ここでE/E/PE安全関連系とは、電気・電子・プログラマブル電子による安全関連系の略で、プログラマブル電子とは、ソフトウエアを含むコンピュータやPLC（Programmable Logic Controller：プログラマブルロジックコントローラ）のことを意味している。ここでは、機械式安全系のことは対象としていない。

前述の定義で「正常な機能に依存する」という言葉が出てくるが、機能安全ではこれが最も重要な概念である。これまでの解説では「正しく機能する」等と書かれていることに相当する。これらは、「正しく機能する」ことで実現される安全機能のことで、正しい機能が失われることもあることを最初から想定している。従って、正しく働くこともあるし、働かないこともあるという確率の概念が最初から入っている。ここで、確率に基づく安全（確率安全）と構造に基づく安全（構造安全）の違いを理解する必要が生じる。構造安全では、機械的に、構造的に壊れないように構築し、壊れ方も予想できるので、どのくらいの確率で壊れたり、故障したりするかということは、あまり、表立って議論はされてこなかった。一方、ソフトウエアを含んでいるコンピュータ等の電気・電子装置は、どのような壊れ方、故障の仕方をするかが予想できないので、どのくらいの確率で正しく働いて安全を確保できるのか（確率安全）ということが重要な指標となる。機能安全では、もちろん、確率安全を対象としている。

最後に、故障は、安全の観点から故障後のシステムの状態によって、二つに分類されることに注意しなければならない。安全側故障と危険側故障である。故障してもシステムの安全が確

保されているものと、システムが危険状態になってしまうものとである。故障しても安全というのは、故障は常に安全側になるようにすればよいので、これを構造的に実現したのがフェールセーフである。機能安全では、故障の存在は認めても、必ずしも危険側故障を無くすことができないので、いかに危険側故障を少なくするかが基本である。機能安全における安全の度合いは、危険側故障に至る確率の少なさで評価される。安全側故障は安全が確保されている状態なので、機能安全では一般的に評価の対象にされていない。

以上、機能安全の考え方について、かなり細かいところまで説明をしてきた。機能安全を正確に理解するために必要な概念のペアを第1表に纏めておく。第1表で、機能安全に関連する概念は、ペアの後者、すなわち、安全機能、付加的に付け加えられた安全機能、制御しているサブシステム（EUC制御系）、安全関連系、電気・電子・プログラマブル電子（E/E/PE）による安全系、確率安全、危険側故障等が、それぞれ対応している。

第1表　機能安全を理解するために必要な概念の主なペア

1	本来機能／安全機能
2	本体に組み込まれている安全機能／付加的に付け加えられた安全機能
3	制御されているサブシステム（被制御系：EUC）／制御しているサブシステム（EUC制御系）
4	非安全関連系／安全関連系
5	機械式安全系／電気・電子・プログラマブル電子（E/E/PE）による安全系
6	構造安全／確率安全
7	安全側故障／危険側故障

機能安全の国際規格IEC 61508の安全の定義では、「全体に関する安全のうちE/E/PE安全関連系及び他リスク軽減措置」という言葉からE/E/PE安全関連系だけでなく機械式安全系も含んでいるのか、付加的に付け加えられた制御系だけなく本体に存在する制御系も含むのか等は不明なところがあり、かなり広く解釈することも可能である。これまでの考察から、現時点では、機能安全とは「システム全体の安全のうち、安全のために付加的に導入されたコンピュータ等の電子制御システムの機能が、正常であることによって達成される安全」とかなり狭く定義するのが、最も適切ではないかと筆者は考えている。参考のために、今までの定義の一覧表を第2表に記しておく。第2表の最後に、本報告で紹介する厚生労働省での検討会の報告書[3]に記されている機能安全の定義を紹介しておく。労働安全という立場から現時点で検討するにあたっては、限定的な定義となっており、妥当な定義であると考えられる。

第2表　機能安全の定義

用語の意味	正しく機能することにより実現される安全機能
もう少し詳しい解説	システムの安全のために付け加えられたサブシステムが、正しく機能することにより、システム全体の安全を確保する機能
もう少し現実的な定義	システムの安全のために、付加的に導入された制御系の機能が正常であることによって達成される安全
IEC 61508による定義[2]	EUC及びEUC制御系の全体に関する安全のうち、E/E/PE安全関連系及び他リスク軽減措置の正常な機能に依存する部分
現実的で適切と考えられる定義	システム全体の安全のうち、安全のために付加的に導入されたコンピュータ等の電子制御システムの機能が、正常であることによって達成される安全
厚生労働省の報告における定義[3]	新たに電子等制御の機能を付加することにより、当該機械等によるリスクを低減するための措置及びその決定方法 注1）電子等制御：機械類等に係る電気・電子プログラマブル電子制御 2）リスク：労働者の就業に係る負傷又は疾病の重篤度及び発生する可能性の度合い

2. 機能安全の使い方

システムの本来機能や性能の高度化のためには、コンピュータ等の電子機器は盛んに使われてきたが、安全に関しては決して積極的でなかった経緯がある。コンピュータのソフトウエアにはバグがつきものであるし、電子機器はどのように壊れるか不確かなので、安心して安全装置としては使えないという主張からである。

しかし、こんな高機能、高性能な機器を安全装置のために使わない手はないという考えから、機能安全が主張され、主として安全制御等を中心に利用されはじめてきた。

この時の機能安全の適用の仕方は、大きなリスクが存在するところには、それなりの危険側故障率の極めて少ない電子制御システム（以後、安全装置という）を使おうという発想である。すなわち、安全装置が故障することは認めるが、危険側故障率の低さという信頼度で評価してクラス分けしておき、被制御系のリスクの大きさに対応したクラスの危険側故障率の安全装置を利用するものである。以下に、機能安全の利用のステップの概略を紹介する。

① 被制御系におけるハザード（危険源）を見出し、そのリスクの大きさを評価する。
② そのハザードのリスクを低減するためには、安全装置で何をどのように制御をすべきかの機能（安全要求機能）を決定する。
③ リスクが許容可能なリスクになるまで低減させるためには、安全装置に対してどのくらいのレベルの危険側故障率が許されるか、性能（要求安全度水準）を決定する。すなわち、そのリスク低減に必要な機能安全のレベルを決定する。
④ 与えられた要求安全度水準を満たすように安全装置を構築して設置する（又は、使用しようとする安全装置がその要求安全度水準を満たしているか否かを判定する）。

ここで注意しなければならないことは、機能安全では、安全装置が正しく機能するという信頼度の高さでハザードのリスク低減に対応していることである。危害の発生頻度の低減の面で貢献しているが、危害の酷さに関する低減には関与していないことである。

以上のステップは、リスクアセスメントの考え方に基づいている。ステップ③の付加する安全装置に対してどのくらいのレベルの危険側故障率が許されるかの性能を表わす要求安全度水準は、通常、許される危険側故障率でランク分けされていてる。IEC 61508[2]では、SIL（Safety Integrity Level）として、SIL1～SIL4の４段階に、ISO 13849-1[1]では、PL（Performance Level）として、a～eの５段階に分けられている。なお、SILは、危険側故障率だけで分類されているが、PLでは、従来の構造による安全装置の類別（カテゴリと呼ばれる）も加味して分類されている。

ここでは詳しく説明するゆとりはないが、SILやPLの詳しい内容、与えられたハザードのリスクに対して、許容可能なリスクにするためには、どのレベルの要求安全度水準が必要かを決める手順、構築しようとしている安全装置が、または与えられた安全装置が、要求安全度水準を満たしているか否かの判定、すなわち、構成サブシステムの信頼度等からシステム全体としての安全装置全体の要求安全度水準をどのように決めていくかという計算方法（この計算には、危険側故障率だけでなく、通常、検査間隔、修理時間、診断範囲、共通原因故障等も考慮される）、等々を知る必要がある。これらの詳しい内容については、各種の参考書、または文献(3)を参照されたい。

なお、危険な機械に対しては、その機械に設置する安全装置には、このレベルの要求安全度水準が必要であると、前もって、安全基準や法規等で決められている場合も多い。

前記のステップ③と④の要求安全度水準が適切に決定されているか否か、及び、実際の安全装置がその水準を満たしているか否か等を製造の当事者ではなく、第三者が専門的な立場から証明する（適合性認定）必要があるが、そのための認定、認証機関の設置は必須であり、欧米等ではすでに適合性認定がは行われているが、我が国では、これから本格的な体制が整備されようとしているところである。

3. 厚労省における機能安全の取り組み

厚生労働省では、これまで労働の現場で使用する機械や設備に関しては、国際安全基準に沿って、「危険性または有害性等の調査等に関す

る指針」や「機械の包括的な安全基準に関する指針」を出しており、機械類の本質的安全設計や機械式等の構造に基づく安全装置等を用いて、機械設備の安全性の水準の確保を行ってきた。労働安全衛生法令による規制も、この方針に沿って行われて来ている。最近、コンピュータ等の電子機器を用いた高度で信頼性の高い安全制御装置が発達し、信頼性に基づいてリスク低減を確保する機能安全の考え方が国際規格として規定され、欧米では、機能安全を規制に取り入れるようになってきている。このような現状を考えて、厚生労働省では、労働安全衛生法令の中でも機能安全が適用できないかを検討するために、「機能安全を用いた機械等の取扱規制のあり方に関する検討会」[3]を設置して、

① 機能安全の要求安全度水準の設定及び適合に関する基準のあり方
② 機能安全の基準を満たす機械等の取扱規制における特例措置のあり方
③ 機能安全に係る第三者機関による適合性認証のあり方

について検討をして、その報告書を公開している[3]。すぐにでも影響があるのは、これまで機械式や構造的な安全装置しか認めていなかった労働安全衛生法令の取扱規制の中で、機能安全の基準を満たす電子制御等による安全装置を用いた場合、どのような特例措置を認めていくか（上記の②の項目）であろう。この件について、報告の中から、いくつかを紹介してみよう。

(1) 機能安全を用いることで、制御装置等の点検・検査等の頻度を緩和できないか

重篤度の大きな機械等（ボイラー、第一種圧力容器、クレーン等の特定機械等）については、制御装置等に対しては資格者の点検が義務付けられているが、要求安全度水準が高くなるに応じて、点検頻度を下げることは妥当であるとしている。相対的に重篤度が低い機械等（構造規格が定められている機械等）に関しては、安全装置等そのものの点検頻度を下げることについて検討する余地がある、としている。

(2) 機械式の安全機能を機能安全に代替できないか

重篤度の大きな機械等に関しては、国際規格でも機械式の安全装置等の省略は認められていないので、労働安全衛生法令でも認められない。しかし、それより相対的に重篤度が低い機械等については、国際規格で機械式の安全装置を電子等制御の安全機能で代替することが認められつつあるので、労働安全衛生法令でも、一定の程度、代替を認めることは可能であろう、としている。

(3) 量に応じて規制が厳しくなっていく安全制御に機能安全を使えないか

労働安全衛生法令では、温度、圧力等の指標が大きくなるに従い、規制が厳しくなる仕組みになっているが、リスクの大きさに応じて要求安全度水準を高くすることで、機械式の安全機能の代わりに電子制御等による安全機能を認めることについては、検討の余地がある、としている。

(4) 遠隔制御に機能安全は使えないか

通信機器等に関しては機能安全を用いる必要があるが、機械等本体の機能安全とは、切り離して議論する必要がある、としている。

(5) 型式検定で機能安全は使えないか

国際規格では、要求安全度水準に応じて試験の一部を省略することを認めているものもあり、労働安全衛生法令の型式検定でも、同様の措置が可能かを検討する余地がある、としている。

以上の中にも、厚労省としてやろうと思えばすぐにでも適用可能な施策もある。例えば、ボイラーや産業用ロボット等の分野で機能安全が取扱規制の中にすぐにでも出てくる可能性があるので、注視していく必要がある。

おわりに

現在の労働安全衛生法令では、従来の機械安全の立場から機械設備を規制してきた。すなわち、安全装置の基本は機械式であるとしていて、

安全制御の厳しさの度合いは、リスクの大きさに応じてカテゴリーといわれる構造として規制してきた。そこには表だっては確率という言葉は用いられていなかったが、安全制御装置のカテゴリーが高くなるに従い、危険側故障率は小さくなっているはずである。リスクアセスメントに基づいて許容可能な安全を確保するのであれば、機械的、構造的な安全装置に対しても、本来的に確率的な評価が入ってくるのは必然である。コンピュータを代表とする電子機器等がここまで高度化してくると、信頼度の評価に基づいて安全を確保するという機能安全の果たす役割は極めて重要になってくる。安全の確保のために構造安全と確率安全とは、信頼性を通じて積極的に融合して考えなければならない時代である。機能安全は、今後、益々その重要性を増し、労働安全衛生法令にも直接、機能安全が導入されるようになるのは時間の問題だろう。ただし、安全設計の基本であるスリーステップメソッドが示すように、本質的安全設計が第一であり、安全防護や安全装置は第二であること、すなわち、機能安全は、確率安全に基づく安全装置の役割であり、その前に考えるべきは本質的安全であって、その中心は構造安全であることを忘れてはならない。

＜参考文献＞
(1) ISO 13849-1（JIS B 9705-1）機械類の安全性－制御システムの安全関連部
(2) IEC 61508（JIS C 0508-4）電気・電子・プログラマブル電子安全関連系の機能安全
(3) 機能安全を用いて機械等の取扱規制のあり方に関する検討会報告書，厚生労働省安全衛生部安全課（2016.3.30）

【筆者紹介】
向殿政男
明治大学　名誉教授

特集：機能安全の現状と動向

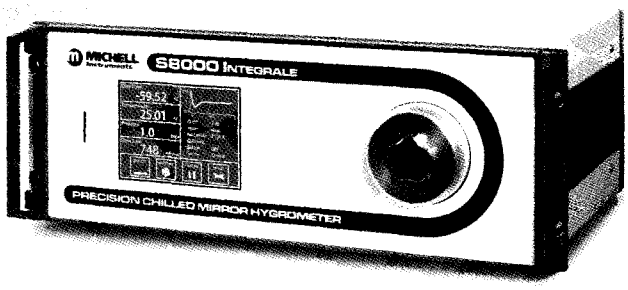
◆平成28年10月5日発行(毎月1回5日発行)
◆第44巻第11号(通巻585号)
発行：日本工業出版 http://www.nikko-pb.co.jp/

2016 10
585. Vol.44. No.11

計測技術
Instrumentation and Automation

英国ミッシェルインストルメンツ社の 最新・次世代製品

最新設計の鏡面冷却式露点基準器
S8000 Integrale mkII
インテグラーレ・マークツー



精度±0.8%RHを達成した
最新・相対湿度センサ
HS3
ハイグロ・スマート3

ポータブル相対湿度バリデータ
HygroCal 100
ハイグロ・キャル100

2016. 10 Vol.44 No.11 特集：機能安全の現状と動向 通巻585号