機械分野の安全目標

○向殿政男（明治大学　名誉教授）

１．機械分野における安全目標の概要

機械分野の安全目標の策定には、二つの考え方が共存している。一つは、構造的な安全目標、すなわち、安全を実現する構造を仕様として決めて目標とする考え方である（これを構造安全の考え方と呼ぼう)。通常の安全基準も、この形の安全目標の一形態と考えることができよう。もう一つは、信頼度に基づく安全目標、すなわち、機械システムが危険な故障を起こす確率や、安全を確保する機構が満たすべき信頼度を数値等として決めて、目標とする考え方である（これを確率安全の考え方と呼ぼう)。前者の構造安全に基づく安全目標の例としては、本質的安全設計（初めから危険源がないように、または、事故の危害のひどさ抑えるようにエネルギーを小さくするような設計等）の要請が典型的なものである。また、フェールセーフ(不具合が生じたら、システムが安全側になる、例えば止まってしまう）ように構成するのもこの例でる。更に、例えば、プレス機械において入口を柵で囲い、柵が降りている時しかプレスは稼働できないようにし、かつプレスが止まっている時にしか柵は上がらない構造に作るというインターロックの要請もこの例である。一方、確率や信頼度に基づく確率安全による安全目標の例としては、例えば、原子炉システムが故障をして放射線が漏れ、近くの住民がガンによって死亡する確率は、１０^{-6}/年以下にするという数値目標は、この例である。更に、ロボットシステムを光カーテンで囲い、人間が光カーテンに触れたらロボットを止める安全装置等が、人が触れても止まらない故障の発生率、すなわち危険側の故障率を１０^{-8}/時間以下にしなければならないといった考え方である。

なお、構造安全でも確率安全でも、明確に構造や数値で記述するのではなくて、その特性や機能を定性的に記述する場合も多い。そのような場合の方が、条件やシステムの特徴による違いを吸収したり、時代の変化に対応しやすいといった点から、現実的である場合が多い。構造安全でいえば、仕様規定ではなく性能規定として、例えば、「部品の一つの故障では、安全機能は損なわれないこと」といった表現が、また、確率安全では、「危害は、考えられない頻度しか発生しないこと」といった表現が用いられる。

構造安全と確率安全の両者は決して無関係ではない。構造を決めてもそれが正しく働く確率が必要になるだろうし、信頼度を決めて目標としてもそれを実現するための構造を如何にするかといった視点は不可欠であるからである。

以上の安全目標に対する構造安全と確率安全の共存は、機械安全の分野だけでなく、多くの安全の分野でも同様と考えられる。機械分野に関しては、特に、構造安全の考え方が最初に提案されていて、最近、機能安全の名称の下に、確率安全の考え方が強く提案されるようになって来ている。

２．カテゴリの考え方：構造安全

機械分野にける安全目標の特徴は、危害のひどさの程度ごとに安全目標を構造として定めていることである。この状況を国際規格 ISO13849-1 (1) (JIS B 9705-1：機械類の安全性－制御システムの安全関連部―第１部設計の一般原則)で見てみる。この規格は、機械における制御システムの安全関連部についての規格である。すなわち、本来の機能を果たしている制御対象の機械に対して、それ

を安全に制御する安全関連部、すなわち安全制御や安全装置等に対する規格である。その重要性に鑑みて(すなわち､それが正しく機能しなかった時の危害のひどさの程度を考慮して)､その構造の目標をカテゴリに分けて掲げて目標としている。カテゴリが大きいほど、機能しなかった時の危害のひどさの程度が大きいとしている。表１は、この形での安全目標を表しているもので、表中で要求事項要約として、あるべき構造が言葉として表されていて、システムの挙動として、その機能が失われて障害が発生した時のシステムの挙動を記している。また、安全性達成のために使用される原則とは､主として安全が信頼度で達成されるのか、構造で達成されるのかについての注釈である。すなわち、カテゴリＢと１は、主としてコンポーネントの信頼性に基づいており､カテゴリ２以降は、構造に基づいて安全が保証されている。

表１：カテゴリと要求事項（ISO 13849-1）(1)

カテゴリ	**要求事項要約**	**システム挙動**	**安全性達成のために使用される原則**
B	コンポーネントのみならずSRP/CS及び／又は保護設備は，予想される影響に耐えるように，関連規格に従って設計，製造，選択，組立，組み合わされること。基本安全原則を用いるこ	障害発生時，安全機能の喪失を招くことがある。	主としてコンポーネントの選択により特徴づけられる。
1	Bの要求事項が適用されること。“十分吟味されたコンポーネント”及び“十分吟味された安全原則”を用いること。	障害発生時，安全機能の喪失を招くことがあるが，発生する確率はカテゴリBより低い。	主として構造により特徴づけられる。
2	Bの要求事項及び“十分吟味された安全原則”の使用が適用されること。安全機能は機械の制御システムにより適切な間隔でチェックされること。	チェックの間の障害の発生が安全機能の喪失を招くことがある。安全機能の喪失はチェックによって検出される。	主として構造により特徴づけられる。
3	Bの要求事項及び“十分吟味された安全原則”の使用が適用されること。安全関連部は次のように設計されていること。 ―いずれの部分の単一障害も安全機能の喪失を招かない。かつ ―合理的に実施可能な場合は常に単一障害が検出される。	単一障害発生時，安全機能が常に機能する。すべてではないが障害のいくつかは検出される。検出されない障害の蓄積で安全機能の喪失を招くことがある。	主として構造により特徴づけられる。
4	Bの要求事項及び“十分吟味された安全原則”の使用が適用されること。 安全関連部は次のように設計されること。 ―いずれの部分の単一の障害も安全機能の喪失を招かない。かつ ―単一障害は，安全機能に対する次の動作要求のとき，又はそれ以前に検出される。それ	障害発生時，安全機能が常に機能する。 蓄積された障害の検出は，安全機能の喪失の可能性を減少する（高DC）。 障害は安全機能の喪失を防止するために適時検出される	主として構造により特徴づけられる。

	が不可能な場合，障害の蓄積が安全機能の喪失を招かないこと。	。	

３．機能安全における安全目標：確率安全

機能安全の規格（IEC 61508）[2] では、安全関連部の役割を、低頻度作業要求モードと、高頻度作業要求又は連続モードに分類して、それぞれの満たすべき機能失敗確率又は危険側故障確率を、安全インテグリティレベル（SIL)として定めている(表２)。ここでは、最も高いSILは４であり、高頻度作業要求又は連続モードにおいて、発生確率が 10^{-8}/時から 10^{-9}/時ということは、約 10^{-5}/年となる。

表２　SIL(安全インテグリティレベル）（IEC 61508)[2]

SIL	低頻度作動要求モード運用（注１）	高頻度作動要求又は連続モード運用（注２）
4	１０$^{-5}$以上１０$^{-4}$未満	１０$^{-9}$以上１０$^{-8}$未満
3	１０$^{-4}$以上１０$^{-3}$未満	１０$^{-8}$以上１０$^{-7}$未満
2	１０$^{-3}$以上１０$^{-2}$未満	１０$^{-7}$以上１０$^{-6}$未満
1	１０$^{-2}$以上１０$^{-1}$未満	１０$^{-6}$以上１０$^{-5}$未満

注1　作動要求当たりの設計上の機能失敗平均確率
注2　単位時間当たりの危険側故障確率[1/時間]

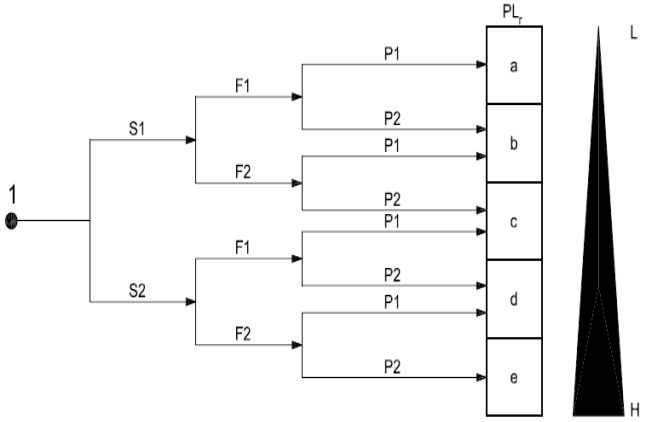
４．構造安全と確率安全の融合

国際安全規格 ISO 13849-1 は、機能安全の影響を受けて 2006 年に改定さて､安全関連部の満たすべき危険側故障の発生率の少なさがパフォーマンスレベル（PL)として示されている(表 3)。図-１に、PL の決定方法の例を示す。これは、リスクの大きさに従い、そのような危害が発生しないようにするために、安全関連部の信頼度の数値を決めているものである｡この各 PL を実現するための構造のランクが表１のカテゴリであるという関係にある｡表１のカテゴリーと表３の PL の関係は､色々な場面や条件を想定して検討をされている。

表３によれば、死亡事故の可能性がある場合に最も大きなリスクとして、それを防ぐための PL は e のレベルである必要があることを示しており、発生確率が 10^{-7}/時から 10^{-8}/時ということは、約 10^{-4}/年となる。PL と SIL の関係の例が表４のように示されている。ここでは、SIL4 に対応する PL のレベルは存在していない。

表３パフォーマンスレベル(PL)(ISO 13849-1)[1]

PL	時間当たりの危険側故障発生の平均確率（PDF）［1/h］
a	$10^{-5} \leqq$ PDF $< 10^{-4}$
b	$3\times10^{-6} \leqq$ PDF $< 10^{-5}$
c	$10^{-6} \leqq$ PDF $< 3\times10^{-6}$
d	$10^{-7} \leqq$ PDF $< 10^{-6}$
e	$10^{-8} \leqq$ PDF $< 10^{-7}$
注記　時間当たりの危険側故障の平均発生確率に加えて，PLを達成するために，他の方策も必要とされる	



図における記号の説明

1　リスク低減に安全機能の寄与度を評価するための開始点

L　リスク低減への寄与度 “低”
H　リスク低減への寄与度 “高”
PLr　要求パフォーマンスレベル
S　傷害のひどさ
S1　軽症（通常，回復可能な傷害）
S2　重傷（通常，回復不可能又は死亡）
F　危険源への暴露頻度及び／又は時間
F1　まれから低頻度，及び／又はさらされる時間が短い
F2　高頻度から連続，及び／又はさらされる時間が長い
P　危険源回避又は危害の制限の可能性
P1　ある条件では可能
P2　ほとんど不可能

図１ 安全機能に対する要求 PL_r 決定のためのリスクグラフ（ISO 13849-1）(1)

表４　パフォーマンスレベル（PL）と安全インテグリティレベル（SIL）との関係（ISO 13849-1）(1)

PL	SIL 高／連続運転モード
a	—
b	1
c	1
d	2
e	3

５．あとがき

カテゴリを中心とした従来の機械分野における安全目標は、構造安全の考え方が中心であった。最近注目を集めている機能安全は、確率安全の考え方が中心となっている。現在、、両者の融合が図られており、現実の安全性確保には、両者は密接にして不可分の関係にある。

ここで紹介したカテゴリ、SIL,PL 等は、現実にはリスクアセスメントの一環として用いられている。すなわち、機械システムの満たすべき安全のレベルが決められた時、機械システムに存在する各危険源に対して、そのリスクの大きさを評価し、許容可能でない場合には、その危険源のリスクの大きさに応じて、適切なカテゴリ、SIL,PL 等の安全方策を施さなければならない、という形で用いられる。

ここで、本来の安全目標、すなわち、機会システム全体の危険側の故障率や許容可能なリスクの大きさは、対象とする危害によって変わるだけでなく、機械安全、製品安全、労働安全等の分野によって、しかも個別のシステムや条件によって変わり、機械分野で全体的に統一した安全目標は見当たらないのが現状である。

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―第１部設計の一般原則)
（２）IEC 61508 (JIS C 0508：電気・電子・プログラマブル電子安全関連系の機能安全の規格