Safety Documents of the National Institute
of Industrial Safety, NIIS–SD–NO.13 (1996)
UDC 62-521：62-783：621.3.07.681.5.09

4. 機械制御回路の安全性評価法

—フェールセーフ性を確認するための故障解析法の提案—

梅崎　重夫*，池田　博康*

4.1 はじめに

近年，国際的に安全問題への関心が高まる中で，機械の製造者が設計段階で適切な安全対策を講じることは，もはや常識となりつつある。特に，欧州では，欧州安全規格ＥＮ９５４－１[1)]（機械の安全性－制御システムの安全に関与する製品設計上の一般原理）でカテゴリ方式による故障対策（機械の危険性が高くなるに従い，より高い水準の故障対策を選択する方法）が義務づけられたこともあり，欧州を市場とする製造者にとって，カテゴリ方式による故障対策の採用は必須となった。また我国でも，平成７年の製造物責任法（ＰＬ法）の施行に伴い，これまで以上に厳格な故障対策を実施する製造者が急増している。

このように，今後の我国では適切な故障対策の実施は必須と考えられるが，故障対策が適切であることを確認するための手法は，我国では，必ずしも十分確立しているとは言えない。そこで，本章では，システムの故障対策（特にフェールセーフ対策）が適切であることを確認するための手法として，ＦＭＥＡを用いた故障解析手法を考案した。以下，この概要について述べる。

なお，ここで故障解析の対象とするのは，原則として，第３章で述べたインタロック機構に限る。

4.2 本章で提案する故障解析の方法

4.2.1 故障の形態と故障モード

工作機械等のインタロック機構は，スイッチ，リレー，電磁弁等の制御機器類や，ＩＣ，トランジスタ，ダイオード，抵抗，コンデンサ，トランス等のさまざまな電子部品類から構成される。これらの機器や部品の故障の形態は，短絡故障，断線故障，劣化故障のいづれかの形態をとる場合が多い。

このうち，短絡故障（ＯＮ故障とも言う）とは，絶縁破壊等によって，電子部品の端子間が導通状態となるような故障を言う。これに対し，断線故障（開放故障またはＯＦＦ故障とも言う）とは，電子部品のリード線や部品間を接続する導線が断線することにより電流が流れなくなる故障である。また劣化故障とは，時間の経過とともに部品の特性が変化するような故障を言う。

短絡故障の典型的な例は，コンデンサやダイオードに定格以上の高電圧が印加されたために，これらの素子が破壊されて導通状態となった場合に見られる。これに対し断線故障の典型的な例は，抵抗やトランスの断線に見られる。

また，劣化故障の典型的な例は，部品の特性定数が時間の経過とともに増加したり減少したりする場合に見られるが，これ以外にも発振器の発振周波数の変化，電磁リレーの応答時間の変化，リレー・シーケンス間のタイミングずれ等を含める場合もある。さらにハンダ付け箇所の接触不良による接触抵抗値の増大や，ハンダ点間の絶縁抵抗の減少などを劣化故障に含めて考えることもある。

一方，インタロック機構の構成要素である安全装置の中には，光軸ずれやレンズの汚れ等によって検知能力が大幅に変動する光線式安全装置のようなものがある。また，マットスイッチでは，断線故障が起こると人体を検出できなくなるものも多い。さらに，他の安全装置でも，機械本体と安全装置の間の配線が短絡や断線を起こしたり，電源電圧の変動（上昇，瞬断，低下等）によって異常な動作をしないとも限らない。

上記のように，インタロック機構で発生する故障モードはさまざまであり，故障解析にあたっては，ま

*機械システム安全研究部　Mechanical and System Safety Research Division

ず発生する可能性のある故障モードを適切に把握する必要がある。**表1**にインタロック機構を構成する電子・制御部品の代表的な故障モードを示す。

なお，電子部品の中には，カーボン抵抗やモールドされたトランスのように通常は断線故障しか起こさないものと，ダイオード，トランジスタ，コンデンサのように通常は断線故障と短絡故障の両方を考えなければならないものがあるから，この点に，特に留意が必要である。

4.2.2　同時多重故障と非同時多重故障

実際の故障解析では，部品の一つだけが故障する場合（単一故障）と，複数の部品が故障する場合（多重故障）に分けて解析を行う必要がある。多重故障には次の2つの形態がある。

(1)　同時多重故障

これは，複数の要素が「同時に」所要の機能を失うことによって発生する故障である。たとえば，電源電圧の変動（上昇・瞬断・低下）によって複数の機器が同時に機能を喪失する場合や，直列接続しているリレーの接点が過電流によって同時に溶着を起こすなどの故障は，これに該当する。

この故障はさらに，共通要因に基づく同時多重故障（単一の原因によって複数の要素が同時に所要の機能を失う故障）と，個別要因に基づく同時多重故障（異なる原因によって複数の要素が同時に所要の機能を失う故障）に分類できる。たとえば，電源電圧の変動がリレー，電磁弁，油圧ポンプ等の数多くの機器に同時に影響を及ぼした場合の故障は，共通要因に基づく同時多重故障に該当する。これに対し，まったく別の原因から，コンデンサとトランジスタがほぼ同時に短絡故障を起こし，これらの相乗効果によって機械が不意作動を起こしたような場合は，個別要因に基づく同時多重故障として扱う。

(2)　非同時多重故障

これは，最初に起こった故障が発見（検出）されずに「潜在」し，その後に他の故障が発生したときに，これら2つの故障が複合的に作用して機械の危険な動作を起こすような故障である。

たとえば**図1**のような回路では，接点ｒ1が溶着を起こしても，接点ｒ2が正常に動作している限りは，見かけ上機械の動作は正常となる（ただし，ｒ1とｒ2は二重化された接点であり，正常時にはまったく同じ開閉動作をする）。このとき，故障は当然ながら発見（検出）されない。しかし，この時点で制御回路には接点ｒ1の溶着という故障が「潜在」することになる。さらにその後に接点ｒ2が溶着を起こすと，これら2つの故障が複合的に作用し，機械を停止できないという危険側の故障が生じる。これが，非同時多重故障である。

4.2.3　故障解析の具体例

実際の故障解析を実行するにあたっては，**表2**のようなＦＭＥＡ（Failure Mode Effect Analysis）を用いることが多い。この場合，故障解析は，まず単一故障の分析から始める。表2は，**図2**に示す回路の故障解析である。ここでは，機械の運転開始時（機械の運転をこれから開始する時）と運転継続時（既に機械が運転中）の2つの場合に分けて故障解析を行った。これは，同じ故障が起こっても，各々の場合で故障の影響が異なるためである。

表2からも明かなように，この回路では，仮に起動ボタンＰＳやリレーＲ1の接点（Ｒ1－1）が溶着（ＯＮ故障）を起こしていると，運転開始時にメインスイッチを入れただけで突然機械が起動することがある。また，リレーＲ1の接点（Ｒ1－3）が接触不良（ＯＦＦ故障）を起こしていると，起動ボタンを押しても負作動ブレーキが作動したままとなり，機器破損を起こすことがある。これらは，いづれも単一故障が危険側や機器破損側の故障となる場合である。

これに対し，リレーＲ1の接点（Ｒ1－2）が溶着を起こしても，実際の機械の動作にはなんら影響がないことから，この段階では，安全上の問題は生じない（安全側故障として扱われる）。しかし，仮に（Ｒ1－2）の溶着故障に続いてメインコンタクタの接点（ＢＸ－2）が溶着故障を起こすと，これらの二重故障により，運転開始時にメインスイッチを入れただけで突然機械が起動することがある。これが，非同時多重故障である。

次に，同時二重故障の解析について述べる。**表3**は，図2の回路について個別要因に基づく同時二重故障の解析を行った結果である。たとえば接点（Ｒ1－2）と（ＢＸ－2）が同時に溶着故障を起こすと，危険側故障となることが分かる。従って，実際の故障対策はこのような要素を重点に対策を講じなければならない。

なお，共通要因に基づく同時多重故障は，たとえば過電流や電源電圧の変動のように，数多くの要素に影

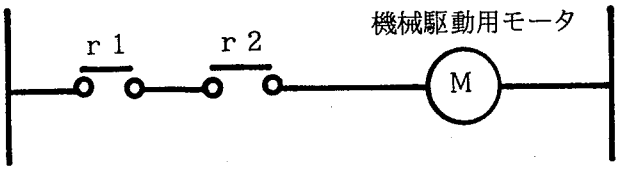


図1　二重化された接点

表1　インタロック機構を構成する電子・制御部品の故障モード

《電子部品類》

区分		故障モード
1	トランス 注1）	・巻線の断線 ・一次側または二次側巻線間の短絡 ・巻線の地絡 ・磁石の割れによる出力の減少
2	抵抗器 注2）	・リード線の断線 ・抵抗体の焼損 ・抵抗値の増加または減少
3	コンデンサ	・リード線の断線 ・絶縁破壊による端子間の短絡 ・静電容量の増加または減少
4	ダイオード	・リード線の断線 ・端子間の短絡 ・逆電流の増加 ・ツェナー電圧の減少
5	トランジスタ	・リード線の断線 ・端子間の短絡 ・逆電流の増加 ・増幅度の増加または減少
6	端子	・端子のゆるみ，接触不良 ・隣接端子間の短絡
7	コネクタ	・コネクタの接触不良 ・隣接端子間の短絡

注1）ケーシングを適切に行っているものは，短絡故障が起こらないものとして扱う。
注2）カーボン抵抗器では，短絡故障や劣化故障による抵抗値の減少は起こらないものとして扱う。

《制御部品類》

区分		故障モード	
8	安全スイッチ類	電気系	・接点の接触不良 ・接点溶着 ・接点の消耗
		機械系	・バネの破損 ・摺動部固着 ・ドグの位置ずれ ・取り付け部のゆるみ
9	電磁リレー	電気系	・接点の接触不良 ・接点溶着 ・接点の消耗 ・励磁コイルの断線 ・電磁石の吸引力低下
		機械系	・バネの破損 ・バネの脱落 ・摺動部固着 ・電磁石の破損
		その他	・応答時間の変化 ・シーケンスのタイミングずれ
10	ソレノイド	・断線 ・端子間の短絡 ・地絡 ・絶縁不良 ・焼損	
11	電磁弁	・開固着 ・閉固着	

《その他の部品類》

区分		故障モード
12	装置間の配線	・断線 ・導線間の短絡 ・導線の地絡
13	表示装置	・ランプや配線の断線 ・配線の短絡
14	電源	・電圧上昇 ・電圧低下 ・電圧なし ・瞬断

注3）参考例として，主要な故障モードを示したものであり，これ以外にも様々なモードが考えられる。

響を及ぼす要因も含まれるから，故障解析の方法は個々のケース毎に個別に判断する必要がある。このため，ここでは，共通要因に基づく同時多重故障の故障解析法については特に提案を行っていない。

4.3 考察

4.3.1 故障対策における2つの方法

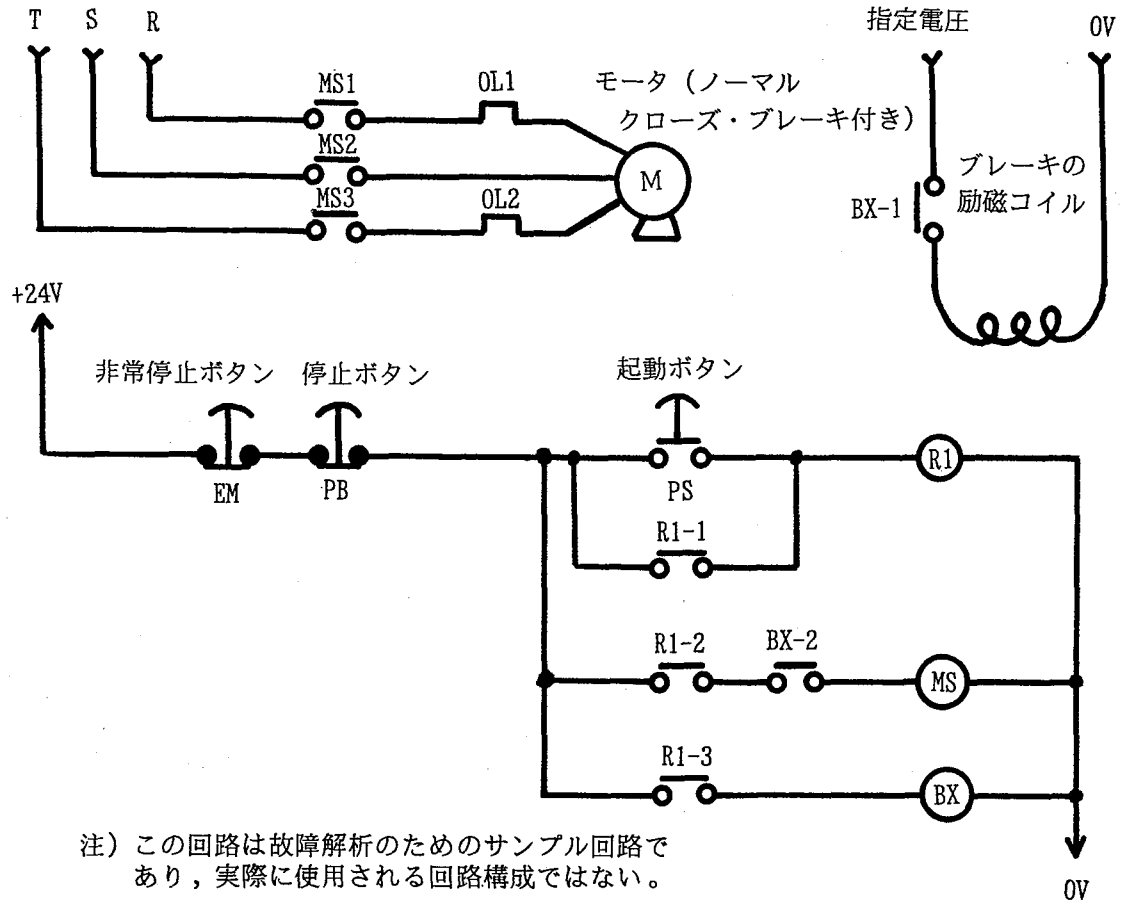
故障とは「システム，機器，部品などが規定の機能を失うこと」[2]である。この現象を確率として表現したのが故障率であり，「ある時点まで動作してきたシステム，機器，部品などが，引き続く単位時間内に故故障を起こす割合」[2]と定義される。

従来，産業安全の分野では，この故障率を減少させることによって，インタロック機構（安全装置や安全のための制御回路）の信頼度を向上させるという対策を講じてきた。実際，きわめて水準の高い我国の信頼性技術をもってすれば，これにより十分な安全水準を達成できる場合も多かったと考えられる。しかし，機器の信頼性が極限にまで到達した今日では，今後とも同様の改善効果が期待できるか否かは疑問である。

例えば，今日，日本の大規模事業場では目標度数率を0.1程度に設定している場合が多いが，これを確実に実現するには，機械側の故障（暴走等）の発生確率は少なくとも10^{-7}回／h以下でなければならない。しかし，現状の機械設備の中にはこの水準を達成できないものも多い。従って，単に故障率だけを減少させても，目標度数率の達成はきわめて困難と考えられる。むしろ筆者らは，今後の故障対策のあり方としては，故障率の「量」的減少とともに，故障の「質」，すなわち「仮に故障が起きても危険側とならないようにする」ための対策が重要と考えている。

この後者の対策の指標として筆者らが提案しているのが危険側移行率[3]である。これは，「発生する全ての故障に対する危険側となる故障の比」と定義されるものであり，システムのフェールセーフ性を評価する際の指標として重要な役割を担う。

ここで，上記2つの指標を使用して，安全上問題となる危険側故障の発生件数を表わすと次式となる。



注）この回路は故障解析のためのサンプル回路であり，実際に使用される回路構成ではない。

図2　故障解析の対象とした再起動防止回路

表２　単一故障と非同時二重故障の解析例

《運転開始時》

故障箇所	単一故障				非同時二重故障		
	故障モード	故障結果	故障検出の可否と検出可能時期	判定	故障結果	故障検出の可否と検出可能時期	判定
非常停止装置（ＥＭ）	ＯＦＦ故障	リレーＲ１とメインコンタクタＭＳがＯＮしないため，運転を開始しない。	運転開始時に検出可能	安全側			
	ＯＮ故障	押しボタン操作によって，溶着した接点を引き離すことが可能。	検出不可能	安全側			
起動ボタン（ＰＳ）	ＯＦＦ故障	リレーＲ１がＯＮせず，運転を開始しない。	運転開始時に検出可能	安全側			
	ＯＮ故障	メインスイッチをＯＮしただけで，運転を開始する。	メインスイッチ投入時に検出可能	**危険側①**			
停止ボタン（ＰＢ）	ＯＦＦ故障	リレーＲ１がＯＮせず，運転を開始しない。	運転開始時に検出可能	安全側			
	ＯＮ故障	押しボタン操作によって，溶着した接点を引き離すことが可能。	検出不可能	安全側			
リレーＲ１の励磁コイル	ＯＦＦ故障	リレーＲ１がＯＮせず，運転を開始しない。	運転開始時に検出可能	安全側			
メインコンタクタＭＳの励磁コイル	ＯＦＦ故障	メインコンタクタＭＳがＯＮせず，運転を開始しない。	運転開始時に検出可能	安全側			
メインコンタクタＢＸの励磁コイル	ＯＦＦ故障	ブレーキが作動し，モータ焼損のおそれあり。	運転開始時に検出可能	機器破損			

（続き）

故障箇所	単一故障				非同時二重故障		
	故障モード	故障結果	故障検出の可否と検出可能時期	判定	故障結果	故障検出の可否と検出可能時期	判定
リレーの接点（R1－1）	OFF故障	リレーR1がONせず，運転を開始しない。	運転開始時に検出可能	安全側			
	ON故障	メインスイッチをONしただけで，運転を開始する。	メインスイッチ投入時に検出可能	危険側②			
リレーの接点（R1－2）	OFF故障	メインコンタクタMSがONせず，運転を開始しない。	運転開始時に検出可能	安全側			
	ON故障	影響なし。	検出不可能（潜在故障）	安全側	BX2との二重故障により，メインスイッチをONしただけで，運転を開始する。	運転開始時に検出可能	危険側③
リレーの接点（R1－3）	OFF故障	ブレーキが作動し，モータ焼損のおそれあり。	運転開始時に検出可能	機器破損			
	ON故障	ブレーキが作動しない。	停止操作時に初めて検出可能	危険側④			
メインコンタクタの接点（MS1～3）	OFF故障	モータMが起動せず，運転を開始しない。	運転開始時に検出可能	安全側			
	ON故障	メインスイッチをONしただけで，運転を開始する。	メインスイッチ投入時に検出可能	危険側⑤			
メインコンタクタの接点（BX－1）	OFF故障	ブレーキが作動し，モータ焼損のおそれあり。	運転開始時に検出可能	機器破損			
	ON故障	ブレーキが作動しない。	停止操作時に初めて検出可能	危険側⑥			

（続き）

故障箇所	単一故障				非同時二重故障		
	故障モード	故障結果	故障検出の可否と検出可能時期	判定	故障結果	故障検出の可否と検出可能時期	判定
メインコンタクタの接点（BX－2）	OFF故障	メインコンタクタMSがONせず，運転を開始しない。	運転開始時に検出可能	安全側			
	ON故障	影響なし。	検出不可能（潜在故障）	安全側	R1－2との二重故障により，メインスイッチをONしただけで運転を開始する。	運転開始時に検出可能	危険側⑦
ブレーキの励磁コイル	OFF故障	ブレーキが作動し，モータ焼損のおそれあり。	運転開始時に検出可能	機器破損			

注）非常停止ボタンや停止ボタンの接点に強い溶着が起こると，人間が押しボタン操作をしても，接点を引き離せない場合もある。

《運転継続時》

故障箇所	単一故障				非同時二重故障		
	故障モード	故障結果	故障検出の可否と検出可能時期	判定	故障結果	故障検出の可否と検出可能時期	判定
非常停止装置（EM）	OFF故障	リレーR1とメインコンタクタMSがOFFとなり，運転を停止する。	故障時，直ちに検出可能	安全側			
	ON故障	押しボタン操作によって，溶着した接点を引き離すことが可能。	検出不可能	安全側			
起動ボタン（PS）	OFF故障	影響なし。	次の運転開始時に検出可能	安全側			
	ON故障	停止ボタンを離した後，再び直ちに運転を開始する。	停止操作時に検出可能	危険側①			

（続き）

故障箇所	単一故障				非同時二重故障		
	故障モード	故障結果	故障検出の可否と検出可能時期	判定	故障結果	故障検出の可否と検出可能時期	判定
停止ボタン（ＰＢ）	ＯＦＦ故障	リレーＲ１がＯＦＦとなり，運転を停止する。	故障時，直ちに検出可能	安全側			
	ＯＮ故障	押しボタン操作によって，溶着した接点を引き離すことが可能。	検出不可能	安全側			
リレーＲ１の励磁コイル	ＯＦＦ故障	リレーＲ１がＯＮせず，運転を停止する。	故障時，直ちに検出可能	安全側			
メインコンタクタＭＳの励磁コイル	ＯＦＦ故障	メインコンタクタＭＳがＯＮせず，運転を停止する。	故障時，直ちに検出可能	安全側			
メインコンタクタＢＸの励磁コイル	ＯＦＦ故障	ブレーキが作動し，モータ焼損のおそれあり。	故障時，直ちに検出可能	機器破損			
リレーの接点（Ｒ１－１）	ＯＦＦ故障	リレーＲ１がＯＮせず，運転を停止する。	故障時，直ちに検出可能	安全側			
	ＯＮ故障	停止ボタンを離した後，再び直ちに運転を開始する。	故障時，直ちに検出可能	危険側②			
リレーの接点（Ｒ１－２）	ＯＦＦ故障	メインコンタクタＭＳがＯＮせず，運転を停止する。	故障時，直ちに検出可能	安全側			
	ＯＮ故障	影響なし。	検出不可能（潜在故障）	安全側	ＢＸ２との二重故障により，運転を停止できなくなる。	故障時，直ちに検出可能	危険側③

（続き）

故障箇所	単一故障				非同時二重故障		
	故障モード	故障結果	故障検出の可否と検出可能時期	判定	故障結果	故障検出の可否と検出可能時期	判定
リレーの接点（Ｒ１－３）	ＯＦＦ故障	正規の運転中にブレーキが作動し，モータ焼損のおそれあり。	故障時，直ちに検出可能	機器破損			
	ＯＮ故障	ブレーキが作動しない。	停止操作時に初めて検出可能	危険側④			
メインコンタクタの接点（ＭＳ１～３）	ＯＦＦ故障	モータＭへの通電が停止するため，運転を停止する。	故障時，直ちに検出可能	安全側			
	ＯＮ故障	モータＭに通電したままとなり運転を継続する。	故障時，直ちに検出可能	危険側⑤			
メインコンタクタの接点（ＢＸ－１）	ＯＦＦ故障	正規の運転中にブレーキが作動し，モータ焼損のおそれあり。	故障時，直ちに検出可能	機器破損			
	ＯＮ故障	ブレーキが作動しない。	停止操作時に初めて検出可能	危険側⑥			
メインコンタクタの接点（ＢＸ－２）	ＯＦＦ故障	メインコンタクタＭＳがＯＦＦとなり，運転を停止する。	故障時，直ちに検出可能	安全側			
	ＯＮ故障	影響なし。	検出不可能（潜在故障）	安全側	Ｒ１－２との二重故障により，運転を停止できなくなる。	故障時，直ちに検出可能	危険側⑦
ブレーキの励磁コイル	ＯＦＦ故障	ブレーキが作動し，モータ焼損のおそれあり。	故障時，直ちに検出可能	機器破損			

注）非常停止ボタンや停止ボタンの接点に強い溶着が起こると，人間が押しボタン操作をしても，接点を引き離せない場合もある。

表３　同時二重故障の解析例

《対角線より上方は運転開始時における故障解析》

		非常停止装置（EM）		起動ボタン（PS）		停止ボタン（PB）		リレー（R1－1）		リレー（R1－2）		リレー（R1－3）		メインコンタクタ（MS）		リレー（BX－1）		リレー（BX－2）	
		OFF故障	ON故障	OFF故障	ON故障	OFF故障	ON故障	OFF故障	ON故障	OFF故障	ON故障	OFF故障	ON故障	OFF故障	ON故障	OFF故障	ON故障	OFF故障	ON故障
非常停止装置（EM）	OFF故障	—	—	0A	0A	0A	0A	0A	0A	0A	0A	0A	0A	0A	0A	0A	0A	0A	0A
	ON故障	—	—	0A	1A	0A	0C	0A	1A	0A	0C	M	0C	0A	1A	M	0C	0A	0C
起動ボタン（PS）	OFF故障	0B	0C	—	—	0A	0A	0A	0A	0A	0A	0A	0A	0A	0A	0A	0A	0A	0A
	ON故障	0B	0B	—	—	0A	1A	0A	1A	0A	1A	M	0C	0A	1A	M	0C	0A	0C
停止ボタン（PB）	OFF故障	0B	0B	0B	0B	—	—	0A	0A	0A	0A	0A	0A	0A	0A	0A	0A	0A	0A
	ON故障	0B	0C	0C	1B	—	—	0A	1A	0A	0C	M	0C	0A	1A	M	0C	0A	0C
リレー（R1-1）	OFF故障	0B	0B	0B	0B	0B	0B	—	—	0A	0A	0A	0A	0A	0A	0A	0A	0A	0A
	ON故障	0B	0B	0C	1B	0B	1B	—	—	0A	0C	1A&M	1A	0A	1A	1A&M	1A	0A	1A
リレー（R1-2）	OFF故障	0B	0B	0B	0B	0B	0B	0B	0B	—	—	0A	0A	0A	0A	0A	0A	0A	0A
	ON故障	0B	0C	0C	0B	0B	0C	0B	0C	—	—	M	0C	0A	1A	M	0C	0A	1A
リレー（R1-3）	OFF故障	0B	M	M	M	0B	M	0B	M	0B	M	—	—	0A	1A	M	0C	0A	M
	ON故障	0B	0B	1B	1B	0B	1B	0B	1B	0B	1B	—	—	0A	1A	0C	0C	0A	0C
ﾒｲﾝｺﾝﾀｸﾀ（MS）	OFF故障	0B	0B	0B	0B	0B	0B	0B	0B	0B	0B	0B	0B	—	—	0A	0A	0A	0A
	ON故障	0B	1B	1B	1B	0B	1B	0B	1B	0B	1B	1B	1B	—	—	1A	1A	0A	1A
ﾒｲﾝｺﾝﾀｸﾀ（BX-1）	OFF故障	0B	M	M	1B&M	0B	M	0B	M	0B	M	M	0C	0B	1B	—	—	0A	M
	ON故障	0B	1B	1B	1B	0B	1B	0B	1B	0B	1B	0C	1B	0B	1B	—	—	0A	0C
ﾒｲﾝｺﾝﾀｸﾀ（BX-2）	OFF故障	0B	0B	0B	0B	0B	0B	0B	0B	0B	0B	0B	0B	0B	0B	0B	0B	—	—
	ON故障	0B	0C	0C	1B	0B	1B	0B	1B	0B	1B	1B	1B	0B	1B	M	1B	—	—

《対角線より下方は運転継続時における故障解析》

0A ……機械が運転を開始せず
0B ……機械が運転を停止する
0C ……影響なし
M ……機器破損（モータ焼損）

1A ……メインスイッチを入れたときに機械が突然起動する
1B ……機械が停止しない

注）①リレーの励磁コイルの断線故障は，接点のＯＦＦ故障に含めた。
②ノーマルクローズ・ブレーキの励磁コイルの断線故障は，接点（ＢＸ－１）のＯＦＦ故障に含めた。

$$N_H(t) = N\ [1 - \exp\ (-\int_0^t E_P(t) \cdot \eta(t) dt)]$$
$$\fallingdotseq N \cdot E_P(t) \cdot \eta(t) \cdot \Delta t \qquad (1)$$

ただし，

$N_H(t)$　：危険側故障の発生件数（回）
N　：対象システム数（個）
$E_P(t)$　：故障率（回／h）
$\eta(t)$　：危険側移行率（回／回）
Δt　：経過時間（h）

(1)式は，災害発生件数が故障率と危険側移行率の積として近似的に表現できることを示している。このことは，故障率と危険側移行率の両方を改善することによって，災害発生件数を減少できることを意味する。しかし既に述べたように，故障率の改善だけでは，我国の大規模事業場が目指している目標度数率は達成できない。すなわち，故障率とともに危険側移行率の改善がどうしても必要となる。ここで述べたＦＭＥＡを用いた故障解析手法は，この危険側移行率の改善の程度を確認する際に効果的に利用できると考える。

4.3.2 故障対策とカテゴリ

欧州安全規格では，システムの故障解析を実施するにあたって，ＥＮ1050[4]（機械類の安全性－リスク・アセスメント）に基づいてリスク・アセスメントを行い，この結果を基に故障対策のカテゴリを与える方法を定めている。このような評価方式をとるために，欧州安全規格の下では，一般に機械の危険性が高くなるに従い，より高い水準（カテゴリ）の故障対策を選択することになる。

参考資料５は，ＥＮ954で定めている制御システムのカテゴリである。これは，我国では一般に「機械の危険度に応じて，どの程度まで故障対策を行えばよいか」を示したものと捉えられている。しかし，筆者らが提案している安全確認形の対策からすれば，カテゴリとは「設計者が故障に対する安全確認をどの程度（レベル）まで実施したか」等の意味も含むと考えられる。そこで，ここでは，カテゴリについて別の意味づけを行い，次の６段階に再整理した。

①　レベル１

十分に吟味された信頼性の高い部品を使うことによって，システムの安全を確保していることが確認された水準。部品が故障したとき安全が確保できるかについては，確認していない水準。

②　レベル２

運転開始時または定期的にシステムの正常性を検査（チェック）することによって，システムの安全を確保していることが確認された水準。検査と検査の間に故障が起きたとき安全が確保できるかについては，確認していない水準。

③　レベル３

単一故障が起きたときは常にシステムの安全を確保できるることが確認された水準。同時多重故障や非同時多重故障が起きたときに安全が確保できるかについては，確認していない水準。

④　レベル４

単一故障だけでなく非同時二重故障や非同時三重故障が起きたときでも，安全が確保できることが確認された水準。

⑤　レベル５

単一故障，非同時二重故障，非同時三重故障，同時二重故障のいづれが起きた場合においても安全を確保できることが確認された水準。

⑥　レベル６

単一故障，非同時二重故障，非同時三重故障，同時二重故障，同時三重故障のいづれが起きた場合においても安全を確保できることが確認された水準。これには，**参考資料１**のNo.21に示すフェールセーフＡＮＤゲート[5]がある。この素子の三重故障解析は，文献6)に詳しく述べられている。

以上のうち，レベル１から４は欧州規格における同等のカテゴリにほぼ対応するものであるが，欧州規格では，同時多重故障に対するレベルを明確に定めていないために，これに対する故障対策を施したものの意義が明確とならない。そこで，同時多重故障に対する故障対策の水準として，レベル５と６を新たに提案した。これは，国際規格との整合性を考慮する立場からは必ずしも妥当とは言えないが，同時多重故障を考慮した機器の優位性を評価する意味からは，重要と考えている。

4.4　おわりに

本章では，システムの故障対策が適切であることを確認するための手法として，ＦＭＥＡを用いた故障解析手法を提案した。その概要は次の通りである。

１）故障の形態を，単一故障，同時多重故障，非同時多重故障の３種類に分類し，各々の故障の発生形態を整理した。また，インタロック機構で発生する故障モードを表に整理した。

２）同時多重故障の中には，共通要因に基づく同時多重故障（単一の原因によって複数の要素が同時に所要の機能を失う故障）と，個別要因に基づく同時多重故障（異なる原因によって複数の要素が同時に所要の機能を失う故障）があることを述べた。

３）非同時多重故障では，最初に起こった故障が発見（検出）されずに「潜在」し，その後に他の故障が

発生したときに，これら２つの故障が複合的に作用して，機械の危険な動作を起こすような故障が特に問題であることを示した。

４）再起動防止回路を例に，ＦＭＥＡを用いた故障解析手法を提案し，単一故障，非同時二重故障及び同時二重故障の解析例を示した。

５）インタロック機構で発生する危険側故障の頻度を目標とする水準にまで減少させるには，故障率と共に，危険側移行率の改善が必要であることを示した。

６）欧州規格で提案されているカテゴリの意味には，「設計者が故障に対する安全確認をどの程度（レベル）まで実施したか」という意味もあることを述べ，故障対策のレベルを６段階に再整理した。

ここで示した故障解析の手法は，あくまでも現段階での試論に過ぎないものであり，今後多くの回路を解析して行く中で手法そのものを発展させて行きたいと考えている。この意味で，この提案について，第一線の設計者や生産技術者からの率直な意見を期待する。

参考文献

1）欧州安全規格 prＥＮ954－１（１９９３年版）

2）日本規格協会，JISハンドブック（標準化）（１９９０年版）　pp.117-138

3）杉本・蓬原，安全の原理，機論，530-C （1990） pp.75-82

4）日本機械工業連合会，機械・オートメーションシステムの安全性に関する調査報告書（1995） pp.59-92

5）粂川・杉本・深谷・江川・梅崎・池田・清水・田畠・富田，高齢者向けＭＥ機器の開発・改善に関する特別研究，産業安全研究所特別研究報告，RIIS-SRR-90(1990) pp.46-49

6）小野里・蓬原，多重故障解析結果の一記述方法，第２５回安全工学シンポジウム （1995） pp.355-358

（平成８年３月７日）