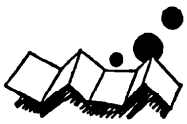
Vol. 29 No. 2　　情　報　処　理　　Feb. 1988

解　説



# ロボットにおける安全確認作業システムの構成†

杉本　旭††　蓬原弘一†††

## 1. 緒　言

文明の発展には危険をともなう場合がある．新幹線，ジャンボ機，原子力，ロボット制御，AT車，……いずれも，より豊かで高度な社会を作り出すための不可欠のシステムであるが，それぞれに危険をともなっている．

現代の文明の進展は，利便享受にきわめて広範な市場をともなう．上に示した文明が市場性，すなわち経済的価値のきわめて高いものであることは言うまでもない．しかし，この経済的価値は努力なしには得られない．そして，その努力は，さらに市場性豊かに，さらに高度に発展させてゆくことに向けられ，しかも，運用コストの低減の要求に答えてゆかざるをえない．設備の製造をするメーカは，この文明の進展とコスト低減という経済の上から相反する要請に猛烈な努力によって答えてきた．この過程で貯えられた技術的イナーシャはきわめて大きい．しかし，その努力の基調とするところは，何よりも経済性である．一方，ユーザからみれば，何よりも安全が不可欠であり，最優先されるべきものである．実は，文明発展の基礎的条件に安全確認が不可欠の要素として入っているのであって，経済優先のメーカは，これをともすれば軽視してしまうのである．

スペースシャトルは，無駄と勝手に判断された安全確認のためのセンサを取り除いて事故に至った．直接の原因となったOリングの交換に対して，技術者に危険の証明をせまった[1]．人に本当の危険が把握できるのなら事故は起こらない．たとえば，自動車の直前を横断することを考えれば分かる．「衝突しそうになったら避ければよい」としてすぐ車の前に飛び出す人はいない．通常，人は明らかに安全と分かるまで，危険をともなう行為を実行しない．スペースシャトルは基礎的な誤りを犯していたことが分かる．

安全が確認されてから実行に移されるべきとする条件は，市場性，すなわち文明の一般大衆への還元という使命により生ずる．一方，安全には「危険を必ず証明することはきわめて難しく，少なくともあらかじめ想定した安全が確認されたとき実行すべし」という基礎的原理が存在する．しかし，ともすれば，この実行が単に難しいという理由だけで見捨てられ，ごまかされる．投資に含まれる賭けの論理は「安全」には通用しない．

著者らは，近年の災害の減少傾向に陰りを生じている事実を憂慮し，従来の安全の抜本的見直し作業を行っている．その結果，フェールセーフ技術を基礎に置く「安全確認型対策」の論理展開を行っている[2),3)]．そこで指向する安全の体系では，作業が安全な状態，危険な状態，あるいは安全とも危険とも分からない「不安」の状態のいずれかの状態で実行されているかを明確にし，「安全」の状態以外では作業の実行を許さない機能を要求し，しかもこれを論理的に正しい構造として達成しようとするものである．ここでは，人間・ロボット系を中心として安全確認型対策における安全確認のための論理的構造を説明する．すなわち，まず，**2.**，**3.** で安全性評価の考え方について述べ，**4.** で，安全確認をともなうシステムの構成要素としてインタロックを導入する．そして，これが安全を十分にまかしうるための徹底したフェールセーフ技術を必要としているため，**5.** で，フェールセーフ技術に基づく安全確認の論理展開を，そして **6.** で，インタロックとフェールセーフ技術のロボットによる実作業への適用について述べる．

† Construction of Safety-Confirmed Operation System in Robotics by Noboru SUGIMOTO (Research Institute of Industrial safety, Ministry of Labour) and Koichi FUTSUHARA (Nippon signal. Co. Ltd.).

†† 労働省産業安全研究所
††† 日本信号(株)

## 2. 信頼性による安全性評価の限界

実際に物を作らない人は，信頼性が高いといわれたことをよりどころにして，安全確認を済ませてしまう．実際に生じた災害をつぶさに調査してきた筆者らの経験から，この典型的機械といえるのがメカトロ機械であるといえる．最先端のメカトロ機械のメーカといえども，その開発に携わる技術者の多くはコンピュータのユーザであり，コンピュータに対して素人である．彼らのよりどころはメーカの提出する根拠の薄い信頼度データである．それにもかかわらず，電子部品のメーカ（何もコンピュータに限らないが）は，たとえば300個の電子部品を1年間試験して1個の故障を生じたなら，その結果を1個の場合に適用して「300年に1回の故障率」という信じられない結論を出しかねない．なぜならいつ交換すべきか結論されていないからである．

安全に係わる論議が混乱をきたしている．特に最近，コンピュータに対する過大な評価が一般化し，こともあろうに安全の分野さえ侵害して，その混乱に拍車を掛けているのである．便利指向のコンピュータに，「人の安全」という責任指向を要求するには(少なくとも現在のマイクロコンピュータの構造を）本質的に変更せざるをえないはずである．

たとえば，ホールド停止しているロボットに近付く場合は，必ずアームを駆動するエネルギを遮断しなければならないが，これはコンピュータによるサーボ停止が「安全」の観点から信用されていないことを示すもので，それはコンピュータの信頼性が低いという理由ではなく，「安全」が信頼性に委ねられていること自体が問題なのである．

生産技術者にとってきわめて重要な信頼度データであっても，根っからの安全管理者や安全技術者は参考にはするが，決してあてにするようなことはしない．故障率を算出すると同じ論法で死亡率などを扱うような人は本当の安全屋にはいない．災害はすべからくレアケースであり，信頼度で表されたデータの裏をかくように，災害は発生するものである．このように信頼度では表現できない事態を対象とするのが「安全の学問」であり，これを技術で達成しようとするのが「安全技術」である．

## 3. 安全の評価指標

作業システムとして安全を論ずる場合，たとえ標準的機械を用いたとしても，これを人間・機械・環境を考慮したシステムとして構成すると，他に二つとない特異性をもつことになり，多数の法則を旨とする論理（たとえば信頼性）は役に立たなくなる．しかも，そのシステムは時々刻々特性を変化させる．

安全作業を保証するシステムはいつ起こるか分からない危険に対処するため，常時安全を確認する手段を必要とする．このためには次の二つの方法が考えられる．

（a）（危険検出型） 危険が発生したとき，それを通報し，システムに停止をかける方法，

（b）（安全確認型） 常時「安全」を通報し，安全が保証できなくなったら，安全の通報を停止する方法(この場合，システムは「安全」の通報による許可信号に基づいて実行されるが，この構成をインタロックという)．

しかし，(a)の危険検出型の方法は危険を検出する手段が故障したとき，これを通報できないまま作業を許す結果をもたらす．これはいわゆる危険側故障の発生を意味するものであり，安全確認のための検出手段として正しい構造とはならない．一般的安全に関する分析法や，時には安全装置の中にさえ，危険を捜し出して(検出して)機械の運用を禁止する（運転を停止する）ものが多い．人間は危険検出型であるから，この方が直感的に理解しやすい．しかし，「危険でなければ安全だ」ということと，「危険が見付からなければ安全だ」というのは同義ではない．工学的に危険検出手段を用意するとき，誤って危険が検出されずに安全と見なして運転を続行するものであってはならない．

これに対して，(b)の安全確認型は安全そのものを検出し，その信号が安全であることの確認をもって運転の許可を与えるものである．安全検出型でなく安全確認型と呼ぶが，これは安全を示す信号の検出と同時に，その信号の処理を行う部分で故障があれば，安全が確認できない事態と見なし，そのときはむしろ「危険」の通報を出力することの重要性を主張している．

このように，安全を保証することは安全側の誤りを保証することであるとすれば，実用的には人間または機械の誤りによる危険の大きさ（危険性）は次式で評価できる．

$$(\text{危険性}) = (\text{誤りの発生率}) \times (\text{危険側移行率}) \times (\text{傷害の大きさ}) \quad (1)$$

ここに，危険側移行率は安全側の誤りを保証する構造によってシステムの危険性を低下させる効果を評価す

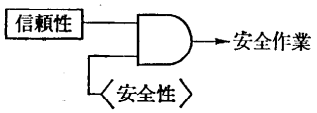



図-1 安全作業システムの構成

るものであり，言い換えれば，危険性を低下させるのに，信頼性に依存しない程度を表す指標である．すでに述べたように，危険がいつ生ずるか分からないとするかぎり，信頼性の追及は安全確保の決定的方法とはならない．そのため，安全の構造を論じて安全性を評価する危険側移行率によってシステムの安全性を代表させることを提案している[4]．すなわち，安全システムは，図-1 に示すように，単なる2重系ではなく，信頼性（機能）が安全性（責任）によってインタロックされる構成となる．ソフトウェアによる自己故障診断などは機能側に位置し，安全の責任を任されるものとはならず，安全確認によるインタロックを必要とする．

## 4. 安全確認の構造

安全確認を事前に完了できるものもある．これを本質安全構造と呼び，危険作業点に作用する力や運動量が人間の許容できる範囲内に抑えられている場合をいう．あるいは力が大きくとも筆者らが開発した非対称アクチュエータ[5]によるオートローダのように，作業する側の力をそのままにして危険側の力だけを抑える構造もこの範ちゅうに入る．しかし，一般に事前の評価によって安全確認を終了できるのはむしろまれである．そこで，安全確認型による安全対策が重要となるが，これは基本的には「安全」であることの証明をともなわないかぎり，危険作業点をもつ機械・環境が作動できない構造（安全確認の構造）を求めるものである．そして，この構造をもつ機械・装置による作業システムを安全確認作業システムと呼ぶことにする．

自動制御の理論体系においては，入力と出力の関係を伝達関数によって表す．そこでは，「情報（あるいは信号）」に基づく普遍的な論議が可能であり，機械系と電気系を特に区別する必要がない．したがって両者は容易に結合され，システムの特性を体系的に論ずることができる．これに対して，安全のこれまでの議論は，危険作業点を直接管理する機械系が中心になされてきたこともあり，領域を越えた理論が発展できなかった．この現状を打破するには，まず安全の原理を明確にする必要がある．そして機械系，電気系を越えて普遍的に「安全」を論ずるための表現法の開発が必

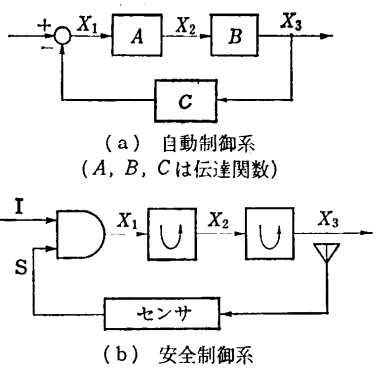



図-2 安全制御系におけるフィードバック
（各要素は安全情報伝達系で，∪ 印はユネイトを示す）

要である．

安全確認型における「安全」では，自動制御と同じく「情報」を扱うが，安全に関わる「情報」のみに注目する．安全に関わる情報を積極的に生成し，その情報が「安全」を示すことを証明し（安全確認の原理に従って安全情報を生成すると表現する），安全情報を後述するユネイト性を保持しつつ伝達し，安全情報が最終的に出力することによって機械の運転の許可（許可信号という）が与えられる．安全情報は誤って「危険」を示す情報に化けること（安全側誤りという）は許されるが，その逆の「危険」を示す情報が「安全」を示す情報に化けること（危険側誤り）は決して許されない．コンピュータによる制御や，人間の操作による作動命令は危険側誤りが存在しうるので，許可情報(信号)によるインタロックの構成を採る．この構成は図-2(b)に示すように，自動制御におけるフィードバック系（図-2(a)）にきわめて類似する．ここではフィードバック情報は出力そのものではなく，出力の影響を含めて，時々刻々変化する環境に対応するための安全情報である．そして，この安全情報は論理積演算要素によって入力と比較される．この構成により入力は危険側誤りの発生が許される．

このように，安全の確認に基づく許可情報によって運転される機械は，許可情報が禁止を命ずるとき，運転を確実に停止しなければならない．これは機械の正しい構造に委ねられる．そして，機械の構造も安全情報を伝達して出力する構成として全く同じ立場で論議が可能である．

多くの場合，緊急時に機械を停止するにはブレーキ装置が必要である．このブレーキ装置は，安全情報の許可に基づき圧縮バネで閉じているブレーキを開放する．安全情報が到達しない場合，エネルギオフによっ

て圧縮バネはブレーキシューを閉じて逆制動トルクを発生させる．安全確認型の論理では，安全情報はエネルギをともなって伝達される．この普遍的な論理は，機械系，電気系，あるいは他の工学系を越えて正しいものであり，安全情報という普遍的特性を介することによって，安全を体系的に論ずることができる．

## 5. フェールセーフ技術

安全確認型の対策は安全の確認を徹底的に行うもので，そのためには，安全情報の生成・伝達・出力のために特別に設計された電子回路やメカニズムが要求される．これらの構造を達成する基礎となるのがフェールセーフ技術であって，これを明確にしておきたい．

フェールセーフとは「故障したとき安全側制御を行う」技術で，常時安全の情報で制御され，故障したとき自ら危険を通報する安全側誤り保障技術である．よく，フォールト・トレラント技術（耐故障技術）の2重系と間違って使われる場合があるが，両者は明確に区別される技術である．これが安全システムとはならないことは，図-1 からも容易に分かる．新幹線の信号システムは2重系である．しかし，安全を維持しているのはフェールセーフであり，2重系は運転の稼動率を向上させる目的で採用されている．

日刊工業新聞社発行の科学技術用語辞典には，「停電や，制御回路，構造構成などの構成要素の故障がその系を操作する人，あるいは近くにいる他の人々を危険にさらすことのないように設計されたシステム」とフェールセーフシステムが説明されている．これを分かりやすくするために，具体的設備の例で説明する．

**図-3** に，家庭の湯沸かし器などで使われるガスの安全供給設備の構成図を示す．人がツマミを押すと弁が開放され，ガスがバーナに供給される．同時に，ライタと同様の点火装置によって着火する．この炎によって熱電対に電流が発生し，この電流が電磁石のコイルを流れることによってツマミの先の接触子が吸引され，弁の開放状態が維持される．もし，着火に失敗したり，何かの原因で火が消えたりすると，熱電対に電流が発生しないので電磁石の吸引力が働かず，弁が閉じて安全が保たれる．すなわち，熱電対から電磁石

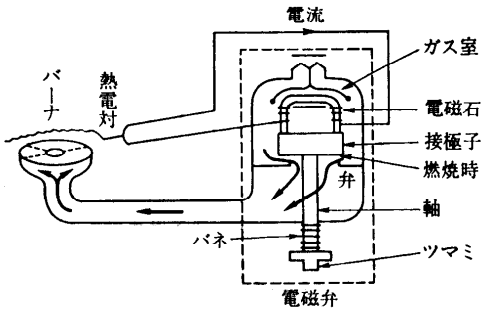



**図-3**　ガス湯沸かし器

による弁（電磁弁）の制御まで安全制御が行われている．

故障を前提として装置を設計する場合，たとえばガス室のケースにひびが入り，ガスを完全に遮断できないという故障を考えると，ここは強固に作る以外に対策はない．ケースは本質的に故障が許されないところである．フェールセーフは，安全が要求される設備にあって，やむなく故障を認めざるをえないところに適用する．

図-3 の電気系は，熱電対，電線，電磁石用コイルのいずれに故障（断線）があっても，電磁石を開放する情報（安全情報）が伝達されない．また，電磁石を構成するコア（鉄心）が壊れても弁開放の電磁エネルギは発生せず，弁が閉じてしまう．したがって，電磁弁開放のための情報は，**図-4** のブロック図で示すように，各要素が正常なときのみ安全の情報（論理値 “1”）として伝達され，故障時この情報が伝達されない特性で表される．これを簡潔に表せば，炎がある（$P$＝“1”）とき弁 $F$ が開放（$F$＝“1”）され，炎がない（$P$＝“0”）とき弁が閉じる（$F$＝“0”）とする制御は，熱電対，電線，電磁石用コイル，電磁石用コアの状態を $K_1$, $K_2$, $K_3$, $K_4$ として，それぞれ正常時を “1”，故障時を “0” で表すと次式となり，すべての要素が正常，すなわち，“1” ときのみ安全制御 $F$＝“1” が実行される（フェールセーフを満たすための基礎的条件）．

$$F = P \cdot K_1 \cdot K_2 \cdot K_3 \cdot K_4 \qquad (1)$$

図-4 においては，伝達される安全情報が弁を開放するためのエネルギとして伝達される．また，実はこの

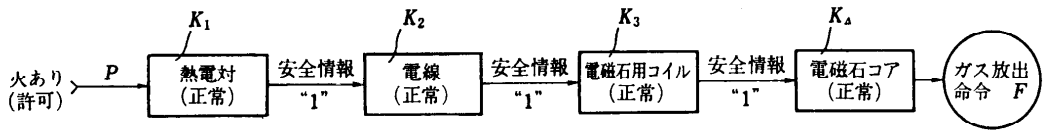



**図-4**　ガス供給制御のユネイト構成

制御系は，トラックなどで利用されている大出力のトランシーバや，近くの工場の大電力電磁スイッチなどで発生する雑音によって誤って弁が開くことがなく，また近くに弁が容易に開くような電源（電池）を有しないことで実現される．すなわち，弁開放のための安全情報の特性を整理すると，次の三つがフェールセーフを実現するための基礎的条件となる．

（1） 安全情報は，エネルギとして伝達される，

（2） 安全情報は周囲に存在する雑音や電源に誤って混触しても安全情報を生じない特性，すなわち，周囲に存在するエネルギレベルより高いエネルギ（ポテンシャル極大の条件と呼ばれる[6]）で伝達される，

（3） 安全情報は非対称誤りの特性をもつ情報伝達要素によって，ユネイトな関係[6]で伝達される．

ここに(2)は，安全情報が機械的に伝達される場合，重力によって弁が開放されてはならないことを意味する．さらに，図-4 を構成する要素は，故障時“0”を出力する（安全情報を伝達しない）特性を有しており，これは非対称誤り（非対称故障）の出力特性と呼ばれる．そして，正常時各要素は入力が安全情報（=“1”）であるとき，出力もまた安全情報（=“1”）を生じ，また，故障によって出力は決して“1”とはならない関係をもつ．これは安全情報伝達のユネイト性と呼ばれる．

## 6. フェールセーフ論理のロボット制御への適用

危険なシステムで安全を保証する制御にフェールセーフが適用される．この制御では「安全です」という安全情報が不可欠であり，情報の扱いには電子回路が利用される場合が多い．しかし，ここではロボットの安全制御用光線式マンセンサに上述のフェールセーフ論理を適用してみる．

フェールセーフで重要なことは，システムを構成する各要素で伝達される安全情報がユネイトな関係で結合され，各要素の出力（あるいは出力換算値）がポテンシャル極大の条件として高エネルギの出力状態となっていることである．

**図-5** は，たとえば右(左)の作業台で人がワーク搬入などの作業を行っていないことを確認して左(右)のロボットによる作業が許可される構成である（シーソーロボット[7]）．**図-6** は，この安全制御の構成である．図-6 で投受光器はマン(人)センサ[8]を構成し，作業領域に張られた光ビームAを人が遮っていないとき

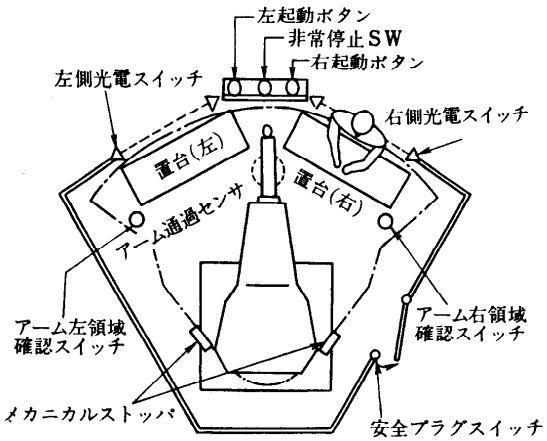



**図-5** シーソ方式における安全確認型の安全手段

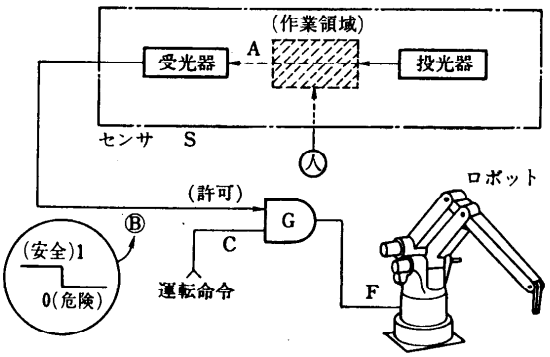



**図-6** ロボットにおける安全制御（インタロック）

運転命令Cが論理積要素Gからロボットへ作業命令Fとして出力される．ここに，論理積要素Gはマンセンサ S から作業許可の信号(安全情報) B があるときのみ運転命令Cを作業命令Fとして発生する判断要素で，当然情報 B と F は図-4 の場合と同様にユネイトな関係でなければならない[3]．そして，判断要素 G は故障で誤って作業命令Fを発生しない特性，すなわち，非対称誤りの出力特性をもつ AND ゲートである．センサSもまた，人が作業領域に存在するにもかかわらず，人の不在情報を発生しない特性，換言すると，人が作業領域に存在しないときのみ安全情報Bを発生する特性（非対称誤りの出力特性）をもつセンサである．

センサ出力は受光器によって発生し，受光器の出力および入力信号は以下の条件で構成されねばならない．

a．出 力 条 件

センサの出力条件Bは，作業領域における人の不在信号を高エネルギ状態で論理値“1”（B=“1”，電圧

あり）として発生しなければならない．

b．入力条件

受光器出力が人の不在信号を論理値“1”とするから，受光器の入力もまた，人の不在時を論理値“1”としなければならない（ユネイトの条件），すなわち，受光器は，人が作業領域にいないとき光ビームのエネルギを受信し，この受光信号をそのまま出力信号として発生させなければならない．ここに，そのままとは否定演算を含まないという意味である．先に図-4 で示したように，安全情報はエネルギとして伝達される．これによる情報の伝達，すなわち，エネルギ発生時を安全とし，零を危険とする情報伝達の特徴は，故障時，零にしか誤らない（非対称誤りの）特性を有する情報伝達に否定演算がないことである（入力“0”を出力“1”にする否定演算では，入力“0”に含まれる故障が出力信号“1”（安全情報）の中に含まれることになって，出力信号は必ずしも安全情報とはならない）．

c．検知ビーム

作業領域も安全情報伝達系を構成するのであって，人の検知信号はこの安全情報に対する作業空間の異常あるいは故障として発生し，このとき，受光器に入力エネルギ零を生ずる構成とする．すなわち，作業空間に入射する光ビームのエネルギは，作業空間が正常であるときのみ安全情報として受光器の入力光（“1”）を発生する構成，すなわち，ユネイトでなければならない．このため，受光器の前方，人が存在しないとき受光できる位置に投光器が配置されることになる．図-7 に示すレーダ構成の光ビームセンサでは，作業領域に入射する光ビーム $i$ では，人が作業領域にいない，すなわち，正常時受光器入力 $r$ が発生せず，逆に人がいるとき $r$ が発生するので，作業領域に入射する光ビームと作業領域から出力される光ビームはユネイトでなく，したがって，フェールセーフシステムとして実現しない[9]．

d．投光器

投光器は故障時光ビームを発生しない特性を有しなければならない．

以上のとおり，センサは正常時のみ安全情報を高エネルギ状態で伝達する構成でなければならず，投光器の出力を $P_T$，作業領域の状態を $K_W$，受光器の状態を $K_r$，受光出力を $B$ とし，投光器，作業領域，受光器の正常状態を“1”，異常時を“0”とおくと，次式となる．

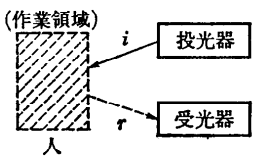


図-7 レーダ方式光ビームセンサ

$$B = P_T \cdot K_W \cdot K_r \qquad (2)$$

ここに，作業領域の状態，すなわち人のあり，なし $K_W \in$（“0” “1”）は，人の作業空間における位置 $x$ に対する受光入力（エネルギ）を $H(x)$，スレショルドを $Th$ とおくとき，次式で示され，外乱光による誤りを防止するためにポテンシャル極大の条件として交流光が利用されねばならない．

$$K_W = \begin{cases} 0, & H(x) < Th \\ 1, & H(x) \geqq Th \end{cases}$$

すなわち，センサにおいてユネイト性は検知空間に対しても適用される．

## 7. 結 言

安全確認型対策における安全確認のプロセスはフェールセーフ技術と，それに基づいて構成されるインタロックによって達成される．フェールセーフの構造を，故障したとき単に OFF 信号を出力するものであるとするなら，“セーブ”の意味は薄い．しかし，安全システムにおいて，一貫して ON 信号を安全，OFF 信号を危険とする許可情報に基づく図-1 のインタロックを確実に実現できるならば，小さな単位のシステム要素のフェールセーフがそのままシステム全体のフェールセーフを決定することになる．安全確認型対策は個々のフェールセーフ性を一貫することが重要である．そのためには，機械，電気を越えて抽象化された論議が必要であり，この場合，「安全情報」が一貫性を担うプロポティである．

筆者らは，この論理に基づいた多くの装置やシステムを開発してきているが，これらは技術的に高度なものばかりではない．しかし，一般に「難しい」として安易に見捨てられてきたものであった．安全技術と他の技術のは行性は今や致命的な状態にある．安全技術のイナーシャは一般的にはきわめて小さいまま取り残されているのである．安全技術はきわめて論理的な技術であり，「技術大好き」の技術者の能力をもってすれば，安全技術のは行性は容易に解消でき，さらに大きな技術的イナーシャさえも期待できると思われる．

## 参 考 文 献

1) 近藤：安全性に係わるマン・システム・インターフェイス，電子情報通信学会技術研究報告

S 87-2, 2 (1987-8).
2) 蓬原，杉本，向殿：安全制御の原理，昭和62年電気学会産業応用部門全国大会，171 (1987-8) (論文誌投稿中).
3) 蓬原，杉本，向殿：安全作業システムにおけるインターロックの構造と実現，電気学会論文誌D 107-9 1099 (1987-9).
4) 杉本，粂川，芳司，蓬原：安全対策の基本構造について，第19回安全工学研究発表会講演予稿集1 (1986-12).
5) 杉本，清水，芳司：非対称アクチュエータによるハンドリングの本質安全，第4回日本ロボット学会学術講演会，497 (1986-12).
6) 川西：Fail-safe，電気学会誌 IM-85-28 (1986-12).
7) 杉本，蓬原：産業用ロボットと安全の論理，電気学会生産設備管理研究会資料 PFC-87-2 (1987-3).
8) 杉本，蓬原：ロボット制御における安全運転用光センサ，第16回安全工学国内シンポジウム 4 PF 9 (1974-4).
9) Sugimoto, Futsuhara : Safety and Technology of Safety Confirmation Type-Coordination with Robots, Trends in Ergonomics/Human Factors IV, Part A 521 (1987-6).

(昭和62年10月5日受付)