５９

安全工学研究連絡委員会報告

社会の安全・安定化への道の確立について

－安全工学の立場から－

平成９年６月２０日

日本学術会議
安全工学研究連絡委員会

この報告は、第１６期日本学術会議安全工学研究連絡委員会の審議結果を取りまとめ発表するものである。

委員長　柴　田　　碧　（地震予知総合研究振興会副首席主任研究員）
幹　事　田　村　昌　三　（東京大学大学院工学系研究科・工学部教授）
　　杉　本　　旭　（労働省産業安全研究所主任研究官）
委　員　板　垣　　浩　（横浜国立大学工学部教授）
　　大久保　堯　夫　（日本大学生産工学部教授）
　　大　音　　透　（いわき明星大学理工学部教授）
　　垣　本　由紀子　（鹿児島県立短期大学商経学科教授）
　　小　林　英　男　（東京工業大学工学部教授）
　　佐　藤　　豪　（第５部会員、慶應義塾大学名誉教授）
　　菅　原　進　一　（東京大学大学院工学系研究科・工学部教授）
　　長　　尚　（信州大学工学部教授）
　　平　野　敏　右　（東京大学大学院工学系研究科・工学部教授）

社会の安全・安定化への道の確立について
－安全工学の立場から－
要　旨

要旨

安全工学研究連絡委員会は，第 16 期　日本学術会議・活動計画に則り，我が国の社会の安全・安定化を図り，国際情勢に基づくものとして確立する方策について，以下のように提言するものである。これは第 14 期以来，引き続き検討を続けてきた本課題に，偶々1995 年 1 月，阪神淡路大震災及び 3 月のオウム真理教問題で社会の不安が増大したのを機に，改めて討議を行った結果をまとめたものである。この討議に当たっては，毎年開催されて来ている安全工学シンポジウム，及びほぼ 1 年半間隔で開催されてる公開の安全工学ワークショップの場で，関連技術者・科学者が中心となり，一般市民も混え講演発表・パネルなどの形で討論を含めて検討して来た成果を参考とした。この際，さらに広い立場からの批判・検討を求めるべく，委員会対外報告として取りまとめた。以下はその骨子である。

提言 1　社会の安全を確保し，その安定化を行うことは，工学の一つの責務であり，その方法論につき他分野と協力しつつ検討し，確立しなければならない。

提言 2　社会の安全を確保するためには，個々人の安全はもちろん重要であるが，それをシステム化し，群としての安全を確保するための論理的研究が必要である。

提言 3　個々人の安全から，群としての安全を得るためには，幼稚園・小学校レベルから研究者・社会人レベルに至るまでの組織的な個人教育・集団教育が必要である。

提言 4　社会の安全を確保し，リスクを低減するためには，国際的な研究の発展からそのシステム化・国際規格化が必要であり，そのための国際研究連絡機関の確立を我が国が中心となって図るべきである。

総論と提言

1. 提言への道

本報告は対外報告として，安全工学研究連絡委員会が，社会の安全・安定化への道を如何に確立するかを検討した結果を第5部の目標とするパラダイムの変換の方針に従い従来の安全工学の立場を離れて第16期末を目途にまとめたものである。

第26回（1996年）安全工学シンポジウムは，従来の6学会の幹事学会（建築・土木・電気・機械・化学・安全工学）に新たに日本人間工学会を加えて，社会不安，リスクについてを主テーマとすることで，1995年の阪神・淡路大震災による社会不安，それに続くオウム真理教問題など，いわゆるバブル期に続く今，社会の情勢は，きわめて不安定であることを踏まえて行われた。この問題は1990年代初めからある意味で予測された。安全工学研究連絡委員会はこの問題を主テーマとし，従来からその活動を行って来た。第26回シンポジウムの実施に当たって，改めて次のようなメモを作成した。

「個人から社会，それも全地球的規模に至るまで，その各々のレベルでの安全問題がある。その場合，安全とはどのように捉えればよいであろうか。常時安全を保つには，発生する可能性のある危害を如何に防止するかにあり，安全工学もそれへ向けての努力を行っている。しかし，現実としての一つの見方として，日常性の中断ということが挙げられる。個人にしても全地球的社会にしても，日常の生活は日々若干は異なっているが，しかし，何日も，何ヶ月も，何年も同じことの繰返しであり，それが人々の生活の安定観のもととなっている。

家庭内事故から自然災害，そして小惑星の衝突まで，このような事件は個人からある都市の住民，そして地球上の人類の日常の生活を，ある瞬間から突然破壊し，1分後，10分後，1時間後，明日に予定していたことをすべて変えてしまう。」

従来，本委員会が継続的に主催して来，本年（1997年）で第27回になる安全工学シンポジウムは，燃焼・爆発と労働災害に主体をおいて出発し，発展して来ている。そして，第20回（1990年）頃より安全を制御するという立場に移りつつ，その領域を拡げるよう努力してきた。それを，さらに社会不安という切り口で新たに捉え直そうとしている。本来，危険・災害は自ずと存在するが，安全は努力して得られるものである。そのメカニズムがわからないものほど，社会不安を惹起し，さらに，同時，広範囲，多発などにより社会全体を不安定なものにする。そして，このようなものは一般に対策が樹て難い。本研究連絡委員会が目指している，単純な安全工学からより複雑なものへとの進展がそこにある。

これを言葉を換えていうならば，“社会安定化工学”ともいうべきものである。簡単にその内容を要約するなら，社会のリスクを積極的に除去することについての方法論を工学としての立場から検討する。社会リスク回避工学ともいえる。広い意味の安全工学の一部であるが，通常の安全工学とは個人に対する危害の回避についての諸論議が中心である。この分野，社会安定化工学とは，あくまで個人の挙動に拠るところからスタートするが，個人が群となって社会を構成したときの，相互の干渉による社会全体の動きの安定化を図り，その安全を目指すものである。サリン事件のような社会不安発生の防止，自然災害の防止などが昨今の話題であるが，原子力災害時の地域防災計画とか，地震時の早期警報システムのように現在進行しつつある各種の行政施策やプロジェクトとも関連がある。また当然，工場従業員の環境管理，被曝管理のような労働科学とも関連する集団行動の問題もこれに含まれる。

従来の安全工学は人間工学同様，個人の行動，特性などを中心に研究され，対策なども論じられて来た。これらは今後とも重要ではあるが，群としての人間と社会を含んだシステムとの間のインターフェースがより新しく重要な問題となりつつある。ここでは社会安定化工学，あるいは社会リスク回避工学ともいえるが，小さい場合は大きなシステム内の数名の集団から，企業集団，さらに大は一都市，一国家のサイズのレベルまで，個々人の特性を基に，それを総合化して，そこで生じるような総合的リスクを回避し安定化するために，必要な科学とその具体化としての工学について研究し，その方法論を確立する。これが現在，社会から要求されている安全工学の拡張，発展であり，パラダイムの変換であるといえる。本研究連絡委員会はこの方向にむけて活動を展開しつつあり，この展開にむけ，我が国の政策・行政の支持を求めるものである。

2. 安全工学の公開性と社会からの受容

上記のように安全工学を社会の内に位置付けたとき，その公開性と具体的な実施が重要になる。そして社会で具体的に実施するためには，社会の一般構成員がよく理解することが重要である。その際の一つの問題点が確率論的考え方の存在である。これに対立するものが鉄道信号で代表される安全確保の方式，フェール・セーフなどで表現される決定論的手法である。航空機の保守などは確率論的であり，構造信頼性につながる。この両者は社会が発展し，複雑化するに従い確率論へと進みつつあるが，決定論のほうが一般の工学者や人々にもなじみやすい。確率論的表現による具体的な目標として，“Safety Goal”など，一応，人々を納得させることができたとしても，たとえば，「もんじゅ」のようなことが起きると，通常の原子力発電所の建設にまで大きな打撃を与え，決定論的安全が如何に世の中で求められているかがわかる。しかし，その一方で空路による旅行，航空機は，確率論をベースとした管理体制で社会的ポジションが得られ，日常生活に受け入れられている。この二つの考え方は，安全工学と社会との関わり合いの根本にあるが，必ずしもどちらというものではなく，社会として両方に対する受容性がある反面，国，民族などで差があると思われる。

上記のことを踏まえて，下記の4項目の提言を行う。

提言 1 社会の安全を確保し，その安定化を行うことは，工学の一つの責務であり，その方法論につき他分野と協力しつつ検討し，確立しなければならない。

現在までの安全工学，とくにその中で重要な役割を占めている人間工学は，個人の問題を扱って来た。しかし，社会が複雑になって来ると，個人の問題の集積だけでは社会の安全を保つ，ないしは安定化を行うことが困難になって来ている。第 15 期に「巨大システムと人間」特別委員会があったが，巨大システムを技術的なものに限定しても，なおかつ現在の巨大社会と無縁ではあり得ないとした。オウム真理教によるサリン事件などは，超能力などに一般社会の構成員，とくに若年層が関心をいだいた当然の結果であり，科学を否定する心と，科学を駆使してサリンのような毒物を作る工学的な心とが同一人の中に潜在している。これは決して，上述の団体に属する個人特有のものでなく，近年の社会全般の風潮である。そのような不安定な状況を打破し，社会全般の安定化を図ることは，工学教育の一部であり，工学者の倫理による裏付けが必要である。

阪神淡路大震災における設計・施工の欠陥は，たとえ，地震そのものが一般的な工学の常

識を超えるものであったにせよ，各種耐震設計基準が，経済的に妥協していた面により拡大助長されて，あのような災害を引き起こしたものといえる。

最近の原子力関係の事故に付随する諸問題も，技術的な事故想定の不十分さと，それに対応する管理態度の倫理性の欠如によるものといえる。

工学は社会を安全なものとし，社会の構成員の人心の安定化を図る責務がある。

提言 2　社会の安全を確保するためには，個々人の安全はもちろん重要であるが，それをシステム化し，群としての安全を確保するための論理的研究が必要である。

提言 1 で述べたように，社会の安全に関与する工学技術者の倫理・努力が重要である。しかしながら，工学技術者が，ただ直観ないしは倫理観で如何ように努力しても，安全を計る対象装置の安全システムの論理が確立していなければ，意味がない。ただ精神訓話的に「安全はなんとか－－－」と駅のアナウンスで繰返すように放送したり，企業で始業前の訓示で述べ，声を合わせてそれを反復したりしても，基本となる安全システムが確立していなければ，人間の本質からみて，努力だけで安全を維持することには限界がある。このことは多くの事例で知られている通りである。

このことを前提に提言 2，提言 3 がある。このようにして，個々人の能力の限界を高めることで，社会全体の安全は成り立つのであるが，しかしながら個々人の努力のみでは社会全体の安全・安定化を期待することは難しい。群としての構成員全体を考えた安全システムの確保の道を見出すことが必要である。例えば，我が国の地震のように短時間に広域的に社会の機能を麻痺させる外乱に対し，社会が分断された状況下で，相対的に安定を保つには，なお広範囲な領域分野の研究者による持続的研究と，社会態勢の整備が必要である。このとは，地震のような天災に限らず，幸いにして，我が国では余り経験はしていないが，多発的な事件に対するものとしても重要である。たとえば O-157 の多発や，往年のスペイン風邪のようなものなどについても，同様な事がいえる。

提言 3　個々人の安全から，群としての安全を得るためには，幼稚園・小学校レベルから研究者・社会人レベルに至るまでの組織的な個人教育・集団教育が必要である。

上述のようなことに際し，社会の安全システムにその構成員が適応し，行動できるようにするためには，その安全の基本から社会的安全システムに至るまでの，幼児期からの教育が必要である。ただ，単に自分の身を守るための安全教育や，職業的知識としての教育ももちろん重要であるが，幼児期から専門教育，職業教育を受ける時期までを通して，いわゆる安全文化を身につけ，本能的にも，倫理的にも，自ずと必要な思考，行動が行われるようにならなければならない。

提言 4　社会の安全を確保し，リスクを低減するためには，国際的な研究の発展から，そのシステム化・国際規格化が必要であり，そのための国際研究連絡機関の確立を我が国が中心となって図るべきである。

安全教育の基本となり，それによって身について行く一般社会の構成員の安全文化，倫理感はその構成員の属する社会，宗教などで異なることは当然である。しかし，社会の安全・安定化を図るための基本事項は世界共通である。現在，ISO*などにより，そのための国際規格化が進められ，時には貿易商取引の条件となりつつある。規格や資格で，上述のような安全の基本となる事柄を拘束しようとすることは，立前上ある程度は必要であるが，この方向に進み過ぎるとかえって形式主義となり，その本質が見失われることになり兼ねない。

ISO などの現行の考え方は，ヨーロッパ的な形式論理的な面が強く，アメリカ的な実務主義とも異なり，我が国などの倫理的基礎のものとも異なる。したがって，これを統合し，より人間性に即した社会の安全・安定化に実効のあるものとしなければならない。その点で，我が国が中心となって，安全工学・科学の国際的な研究連絡機構を作ることは意味があると考えられる。

各論とその展開

本安全工学研究連絡委員会は，このような活動方針に沿って，安全制御（向殿政男 明治大学教授），国際安全研究連絡機構設置準備（平野敏右 東京大学教授を各々の委員長とする）小委員会を設立し，またサブ・グループとして安全教育 S.G.（上原陽一 横浜国立大学名誉教授）を置き，その実施にむけて活動を行って来た。以下その活動に基いて得た具体的な討論内容を各提言との関連において各論として記す。

1. 安全制御の展開と国際規格化

1.1 安全制御と国際的標準化

安全制御の考え方は，以下通常一つの装置について述べられる。このことは社会における事象・機構についても通じるものである。

ある装置の故障がそのまま事故となるようなところは，もともと故障しないように頑強（robust）に作られなければならない。しかし，どうしても故障を認めざるを得ないところでは，故障していないことの確認を常に行い，その確認が得られない故障時には運転を停止するようにする。例えば，圧力容器は正常な圧力の下では十分に耐えるものでなければならないが，圧力を監視する圧力センサは故障を認めざるを得ない。そのため，圧力センサの正常性を確認し，それが確認できないとき圧力容器への流体の供給を停止する。安全制御システムは，故障で安全が確認できないとき，危険な装置の運転を停止するシステムである。

このような，安全確保の体系化が国際的な視野で急速に進められている。国際規格を作るための基準がＩＥＣ*-Guide51 としてすでに示されており，それによれば，機械（装置・システム）は，必ず危険源(Hazards)を有すると考えなければならず，したがって，その危険源が事故となる可能性，すなわちリスク(Risk)をできる限り小さくすることで安全性の向上が図られる。このリスク低減を図ることが安全対策を講ずるということである。

一方，人の命を扱うという安全の特殊性から，安全対策によるリスク低減の効果は公に立証されなければならない宿命を持っている。これは安全立証と呼ばれ，さらにこのための認証機関が公式に行う安全の立証は特に安全認証と呼ばれる。これまで，リスク低減の効果を，

大きく装置の信頼性向上と人の教育に委ねてきたが，これらによる効果が安全立証として明確に示すことが難しい点で安全対策として正式に認められていない。現実的に，装置の故障や人間のミスによってリスクが発生するものと見なし，故障やミスによって事故が生じない効果を証明することが安全立証として扱われてきた。例えば，欧州統一規格 EN954 によれば，産業機械における事故防止の基本は，危険源に人が誤って接近したとき機械を停止させることであり，その場合，安全対策の信頼度を当てにしないことから，故障したときは人の接近の如何に関わらず機械を停止させるというフェールセーフの構造が成立していることが安全立証の対象である。

このように，人のミスと装置本体や安全装置の故障を認めて，安全を確保できる装置は，列車や工業用ロボットの場合のように，無条件安全の状態が存在するもの，すなわち，止まれば安全が確保できるものであり，最終的安全確保は装置に委ねられる。これに対し，飛んでいる航空機のように，無条件安全の状態が存在しないもの，すなわち本来の機能を果たし続けることによってしか安全を確保できないものは，主として信頼性で対処されてきた。現実に故障があったとき人の操作が必要であり，そのため最終的安全確保は人に委ねられることになる。これら二つを明確に区別し，安全立証できる装置には正しくこれを行って，安易に事故回避の責任を人に押しつけないようにする目的で「CE マーキング」など欧州の安全認証制度がすでにスタートしている。しかし，スタートして間もないが，安全立証を基本とする安全確保の方法の限界が問題となっている。すなわち，コンピュータがこれまでの安全立証の条件で実現されていないにも拘わらず，我々はコンピュータなしではもはやほとんどの装置は制御できないという現実的な問題に直面しているのである。

1.2 コンピュータと安全制御

コンピュータが，いろいろな分野で各種の高度な機能の実現のために使用されており，我々の世界になくてはならない存在になっている。その中で，安全の機能もコンピュータを用いて実現しようという試みも多く行われている。しかし，一方で，「コンピュータに安全を任せるのは危険であり，安易に安全の分野にコンピュータを導入すべきではない」という意見もある。この根拠は，コンピュータを構成しているハードウェアやソフトウェアには予想し難い故障やバグ（欠陥）があり得て，それが危険側に障害を引き起こさないということは保証できないというところにある。特にソフトウェアは膨大なステップのプログラムから構成されており，その中から全てのバグを取り除いて，そこには誤りは存在しないという保証を得るのは事実上不可能であるように思えるからである。

また，欧州統一規格の作成に当たって INRS（フランス安全衛生研究所）では，コンピュータの故障モードを数百万について検討し，故障によって ON 側／OFF 側の出力がほぼ同じ割合で生ずることを確認している。したがって，コンピュータによる装置の制御は，故障で止まる側（安全側）となるという安全立証の点から安全であるとはいえないという結論を与えている。

ところが，実際には，コンピュータの高度な機能を安全の確保のために使用しないことはないと考えられるし，事実，すでに多くの分野で自ずと安全の実現のためにコンピュータは利用されている。そして，実際に十分な安全を確保している多くの例が存在する。また一方では，よく知られているように，コンピュータ内のバグや故障が，人命に危害が及ぶような，また，社会を大混乱に陥らせるような障害を引き起こしている例があるのも事実である。

コンピュータシステムを高信頼度に実現・運用するための指針は存在しても，安全の確保のためにコンピュータをどのように導入すべきかの技術上の指針はこれまであまり検討されて来なかったように思われる。上記のような現状と，安全の確保のためにコンピュータを積

極的に導入することが不可避な将来を考えると，是非とも，安心して使用できる「安全機能実現のためのコンピュータの利用に関する基準」を真剣に検討し，作成することが必要な時期である。そのためには，まず，「安全」の考え方に対する根本的な再検討や，信頼性と安全性との関係の明確化の必要があろう。

1.3 機能的安全性

ここで検討の対象としている「IEC1508 機能的安全：安全関連システム」は，IEC/TC56（工業計測と制御）のもとSC65A（システム関連事項）で検討され，1995年6月に提案されている規格案であり，一般的要件（第1部），電気/電子/プログラマブル電子システムの要件（第2部），ソフトウェアの要件（第3部），定義（第4部），第1部の応用に関する手引き（第5部），第2部及び第3部の応用に関する手引き（第6部），技術に関する文献（第7部）からなっている。

安全確保のためのシステムを安全関連システムと呼び，電子技術を利用したシステム，従来の電磁リレーなどプログラムを内蔵していないハードウェア技術によるシステム，及び柵やガードなどリスク低減設備の三つを組み合わせて実現される。本規格案は，電気/電子/プログラマブル電子システム（E／E／PESと略される）が，安全機能の実現に使われるとき満たすべき要件について述べてある。従って，対象としているのは，安全確保のためのE／E／PESのハードウェアの条件（第2部），ソフトウェアの条件（第3部）であるが，本規格案は，将来，一般の安全関連システムにも適用可能なように，具体的なプログラマブル電子システムの安全の要件を述べる一方で，一般的な記述の内容は抽象度が高く，大きな枠組みの提案ともなっている。

本規格案では，基本的な安全確保の戦略として (1)安全ライフサイクル，(2)安全インテグリティの二つを採用している。

(1) 安全ライフサイクル

安全ライフサイクルとは，総合安全ライフサイクル，E／E／PESハードウェアライフサイクル，及びソフトウェアライフサイクルの三つから構成されている。総合安全ライフサイクルとは，E／E／PESを実現するための総合的ライフサイクルすなわち「初期の構想－設計－製作－運用－保全－廃棄」の全てにわたり，それぞれを安全に関連させたステップとして明確に分けて，それぞれのステップで安全を確保するために何をすべきかを明確にする。そして，並行してそれぞれ立証(Verification)－適合(Validation)－評価(Assessment)の手順を踏むように要請されており，安全立証のこれまでの基本的な考え方を広く取り入れようとしている。また，それぞれのステップでは，入力及び出力が計画(Plan)，要件(Requirement)，記述(Description)，報告(Report)，記録(Log)又は要求仕様(Requirement Specification)等のいずれかとして明確に規定されており，それらを文書として作成するように要請されている。

例えば，総合的安全要件のステップでは，それ以前のステップで出力されている危険源とリスク解析記述を入力とし，総合的安全要件仕様（これは，総合的安全機能要求仕様と総合的安全インテグリティ要求仕様の二つから構成されている）を出力する。この総合的安全要求仕様は，以降の多くのステップで入力として使用される。例えば，第13ステップの総合的安全立証では，入力は，前の第7ステップの出力である総合的安全立証計画とこの総合的安全要求仕様であり，出力は，総合的安全立証報告である。

この総合的安全ライフサイクルは，さらに第9ステップで，E／E／PES（ハードウェア）安全ライフサイクルと，ソフトウェア安全ライフサイクルの二つを含んでいる。これらも総合安全ライフサイクルと同様の構成となっている。

(2) 安全インテグリティ

安全インテグリティとは，本規格案で，「安全関連システムが，全ての定められた状況下で，定められた期間，要求された安全機能を満足に実行する確率」と定義されている。具体的には，対象としている安全関連システムの安全機能に要求する安全インテグリティは四つのレベル（安全インテグリティレベル）に分けられ，実際にどの安全インテグリティレベルを要求すべきかは，現在の社会的，政治的，経済的要因で決まるとされている。なお，安全関連システムは次の二つのモードに分類される。

1) オン・デマンドモードの運用：時々，要求（デマンド）に応じて短時間稼働することを要求されるシステム
2) 連続／高デマンドモードの運用：長時間，ほぼ連続して稼働することが要求されるシステム

本規格案では，「安全」を IEC ガイド 51 にしたがい，「傷害に対する受け入れられないリスクからの解放」と定義している。ここで，リスクとは「傷害を引き起こす危険の発生の可能性の率と，それが発生したときの傷害の過酷さの度合い」と定義しており，リスクとは，危険側の故障の発生確率とそれによって生ずる結果の過酷さの度合いの関数と解釈している。

安全インテグリティレベルは，次のように利用される。

1) 制御対象に存在するリスクを決める。
2) 要求される安全インテグリティレベルに見合ったリスクを決める。
3) 低減すべき最低限のリスクを決める。
4) 実際に低減すべきリスクをＥ／Ｅ／ＰＥＳハードウェア，ソフトウェア，それ以外の安全関連システム，及び外部リスク低減設備のそれぞれに割り当てる。
5) 達成されたリスクの低減により，結果として残されたリスクが 2)のリスク以下であれば“よい”とする。

このリスクのクラスの利用方法は，クラス 1 ならば完全に拒否し，クラス 4 ならば幅広く受け入れ，クラス 2 と 3 の場合は，「合理的な実行可能性の範囲内で，出来る限り低くする（As Low As Reasonaly Practical)」ものとして特に ALARP の原理と呼び，この原理に従うならば，これを受け入れようとするものである。

なお，第 5 部には，安全インテグリティの具体的な求め方が詳しく述べられており，また，第 7 部に具体的な安全機能の実現手法や技術が解説されている。

1.4 安全制御の総合化とコンピュータ

「安全」とは，「人命に危害が及ばないこと」である。本規格案でも，主として人に対する安全を扱うと記している。しかし，システムがある有益な機能を実行していて，しかもそれにある危険源が存在する場合，全てにおいて，完全に又は絶対に「安全」と言うことは事実上あり得ないといえる。

安全に関するシステムには，前述のように大きく分けて 2 種類あると思われる。一つは，列車や工業用ロボットの場合のように，無条件安全の状態が存在するもの，すなわち止まれば安全が確保できるものであり，もう一つは，飛んでいる航空機のように，無条件安全の状態が存在しないもの，すなわち本来の機能を果たし続けることによってしか安全を確保できないものの二つである。狭義のフェールセーフは，前者を対象としており，後者はこれまで主として信頼性で対処されてきた。

フェールセーフといえども絶対に安全であるとは必ずしもいえない。実際には，危険側の障害が起こる可能性は，信じられない程度でしかあり得ないようにすることができるということである。すなわち，故障が発生した場合，無条件安全という安全側に落ち込むように機

構として実現し，危険側の障害が十分無視できる程度にしか発生しないように構成できるということである。

後者のような場合の安全性に，フェールセーフの考え方をそのまま導入するには無理がある。といって，これを信頼性のみで対処するのも問題がある。安全性と信頼性との違いをしっかりと認識した上で，この場合の安全性を議論すべきである。すなわち，障害が発生する確率のみで評価するのではなくて，危険側の障害の発生の確率とそれが起きたときに引き起こされる結果の過酷さの度合いの両方を考えて安全性を評価し，それが社会的にも受け入れられるものであるか否かという立場で，後者の場合の安全性を議論すべきである。これが，本規格案でいう「機能的安全」に相当するものと思われる。

人間は間違えるものであり，コンピュータは予想し難い故障やバグを常に内蔵している。従って，無条件に安全を人間やコンピュータに任せるべきではない。しかし，「無条件安全」が存在しないような「機能的安全」を実現するのに，コンピュータを内蔵したエレクトロニクス装置が有効に利用できることは間違いないが，どのようにしたら安心して使えるのかを与える指針が明確でない。本規格案は，これに対する一つの明確な態度を表明しているといえよう。また，もう一つの本規格案の大きな特徴は前述したように運用のモードを，オン・デマンドモードと連続／高デマンドの二つに分けたところにあるように思われる。そして，ここでは常に生じる問題，すなわち，

1) デマンドがOFFのときに，ONに出来ない障害原因が発生しないか，
2) 反対に，デマンドがONのときにOFFに出来ない障害原因が発生しないか，

に対しては，安全ライフサイクルの保守計画である程度対処するものの，障害の頻度とその結果によるリスク評価が，上記の問題を避けた結果のように思われる。

これが上述した安全ライフサイクルの考え方であり，安全インテグリティの概念である。また，リスクの考え方とその利用法である。

なお，ここではソフトウェアの安全性に関しての詳細は述べなかったが，本規格案では，充分検討しつくされた。いわゆる「枯れたソフトウェア」の仕様を全体的に重視しており，N-バージョンソフトウェア（多様性：Diversity）については推奨しているものの，ハードウェアにおけるランダム故障に対するこれまでの信頼性向上の技術の概念がソフトウェアには当てはまらないことを主張し，バグを前もって入らないように作成するような，また，前もってレヴューしてバグを取り除いておくようなソフトウェア工学の手法を推奨しているのが特徴的である。

1.5 今後の問題と社会の安全・安定化への道

多様な危険源が複雑に絡み合って複雑なリスクを発生しており，また，複雑になってしまったシステムを人間が十分に使いこなせない状況にあり，このこともリスクをさらに増大させる要因となっている。しかし，むしろ本質的な問題は，これらのリスク低減を図るためにコンピュータを導入せざるを得ないが，当のコンピュータがリスク低減手段としての資格を容易には与えられない点である。コンピュータ技術の進歩に期待して，コンピュータがこれまでの安全立証の考えで複雑システムのフェールセーフインターロックの役目を引き継ぐことが出来るようになるのが理想である。しかし明らかにそれは不可能である。今後の安全確保システムは，製品のライフサイクルという視野から，長期的かつ緻密な検討を行うばかりでなく，社会制度として認知するまでに構造化が求められる。安全制御が今後の安全確保システムにおける位置づけを明らかにしようとするとき，本規格案IEC1508は重要な検討課題を与えてくれている。以上，一般的な装置の安全の問題について長々と述べてきたが，これらは社会の安全についても全く同様に考えることができる。とくにコンピュータが社会の

秩序を保つことに深く関与することになって行く現在，すべて社会全体の安全の問題について適用できる。

2 安全教育

2.1 目的

科学技術の実践の場である産業は，システムの巨大化，高度化，複雑化の一途を辿り，これをきちんと管理し，運営するのは容易ではない。このため次々と新しいタイプの事故が発生し，国民の生命や財産に多くの被害を与えている。このために安全技術の開発が必要だが，同時に産業界で働く人達はもちろん，社会の人々全般にわたって，十分な安全教育を行うことが要求される。第1に化学産業の分野について教育問題を述べる。化学産業は，事業所内に危険な物質を大量に扱うことが多く，一旦災害が発生した場合の事業所内外への影響の大きさは他の産業の比ではない。ここでは，化学産業に絞ってこの問題をとり挙げる。

第2に技術に関して次の時代を担う世代に対する安全教育を，学校教育でどのような形で実行するかを検討した。

このことは，現代社会は工業化社会であり，ここで我々は計り知れない利便を享受しているが，同時に各種のリスクも背負い込んでいる。社会全般のリスクを低減することの一つに，家庭へ大量に導入されている化学物質についての消費者教育に触れる。

2.2 化学産業における安全教育

2.2.1 概要

化学系企業の新入社員は，技術に関する基礎教育は受けているが，実際のプラントの運転に関する知識の持ち合わせはない。また，安全に関する教育も受けていないことが多い。この人達を教育し，オペレータあるいは管理技術者としなければならない。事業所では技術を安全問題を含みながら教育せねばならない。

現場技術者は次の職務に精通せねばならない。①プロセス運転管理，②設備管理，③保安安全管理，及び④生産管理。最後の二つが運転技術の集約である。これらに関する基礎知識を十分に持ち合わせるだけの教育が必要である。さらに設備改善に関する技術力も求められる。現在の日本の職場ではどこでも，化学工業に限らず，小集団活動や提案制度による設備改善，運転技術改善，保安安全規則の改善，その他種々の改善活動がなされているが，これらは運転管理及び設備管理の実践の結果と強く結びついている。

また，万一事故が発生した際の通報，事故処理，自己記録などについても上述の職務と共通するが，これらに精通し，どのような事態にあっても適確に実践できるよう教育・訓練が必要である。

2.2.2 安全教育の内容

安全に限定すると，教育内容は次のとおりである。

第1部　安全の基礎

①教育のねらい，②安全に関する基本方針，③安全第一ということ，④安全第一を妨げるもの，⑤安全の視点，⑥ハインリッヒ（Heinrich）の法則*，⑦行動災害とプロセス災害，⑧行動災害の起こる仕組み，⑨合理と非合理，⑩組合せによる安全対策，⑪法による安全，

第2部　安全意識の養成

①人間の特性，②大脳生理学による人間の状態，③不注意物語，④盲点を防ぐ，⑤判断を誤らせる盲点，⑥行動を誤らせる盲点，⑦災害事例研究，

第3部　安全対策

①災害の想定，②オペラビリティ・スタディ（Operability Study）*，③ＦＴＡ*，④ＥＴＡ*，⑤安全対策の改善，⑥安全水準の評価，⑦安全に対する努力の評価，⑧安全診断，⑨モデル工場における実施例。

なお，第3部についてはオペレータとして知る必要があるかどうか，国によっては異論がある。この問題は，オペレータを含んだ技術者の倫理という観点で最近論議されている。

2.2.3　上級管理者への教育

以上見られたように，我が国では実際の機器の運転に当たるオペレーターの教育には，相当な力が入れられている。下級技術者の教育も，ほぼこれと同様でかなり高級なことも含め，日常行われている。しかし，上級管理者，経営陣とくに社長クラスに対する教育がどのように行われているのか明確でない。社長など，企業のリーダを含む上級管理者の安全教育の体系化と，その倫理の確立が，今後の大きい課題である。

2.3　学校教育

2.3.1　小／中／高校における教育

学校教育はすべての教育の基本であり，従って，安全教育もまた学校教育の中で実施することが重要である。それは，科学的知識を生活に役立てる，生活のあり方を考える，環境に配慮するといった視点から行われるべきである。最初に示した自動車事故や家庭内化学品の取り入れに関しても，単に危険を避けるという点の教育は，幼稚園から低学年の段階で終了し，生活する上で必要な安全に関する知識を積極的に学習させる方向に進むべきである。リスクの本質を理解させ，自動車や化学品を十分に利用するための知識伝達を行うべきである。安全教育を現在の文化や文明の否定のみに終わらせてはならない。

学校においてこのような安全教育を推進するために，指導者用テキスト，生徒用テキスト，副読本，視聴覚教材などの必要な資料を準備し，教師が教えやすい環境を整える必要があり，同時に安全教育のできる教師を養成することが大切である。

安全教育の中に，内容のある防災教育も取り入れ，とかくおざなりに行われやすいドリルのような避難訓練だけというのではなく，総合教育の一環として取り組むのも効果的である。地震や火山噴火などのメカニズムについての自然科学的説明，化学物質の有用性と危険性及び自動車や道路管理についての工学的説明，避難行動，パニックや危機管理についての社会科学に基づく解説，災害ボランティアなど現実の災害で問題となったトピックスなどが安全教育の中に盛り込まれればより効果的な教育ができる。もちろん実技編として避難訓練などのいわゆるドリル的な防災訓練があることも望ましい。安全教育の中で，災害リスクと安全対策を総合的に理解させるのに，もっと多くの時間を費やすべきである。現在の学校教育は，あまりに受験科目に偏重しており，人間が如何に生きるべきかについての突っ込みが足りなさすぎる。

2.3.2　大学教育

大学生，とくに技術系学生は，将来のますます複雑化，多様化する科学技術の担い手であり，技術を安全性と調和のとれたものとするために，安全に関する基本的な教育を必要とする。これまでの学生は，安全教育を受けていないため，技術系学部の卒業生は，従来，ものをつくるという立場でしか物事を見ないという共通の欠陥を持っていた。これは製造者優先の視点であり，使用者や消費者の立場を考慮しない立場であった。先に自動車事故の原因を，運転者のみに起因させるべきかと述べたのは，このことを考慮したからである。化学プラントの事故で，オペレータの行動に原因があるとされる場合でも，少し調べると設計上に問題があることが多い。

大学生が安全に関する教育を受ける目的は三つある。一つは上述のとおりで，安全のフィロソフィと基礎技術をしっかりと身につけて卒業することである。もう一つは自らを守るためのもので，学生実験，卒業研究，修士及び博士論文作成のための実験を安全に行う方法の実践的技術の習得である。さらに，安全性評価や安全技術の開発ができる高度な安全の専門知識を持った専門家の養成も重要である。

日本学術会議の要請で，国公立の有名大学の化学実験室を査察した日本の化学系企業の環境保安担当者は，その内容の余りの貧弱さにショックを受けた。いくら学生が実験に対する安全技術を習得しても，設備そのものが整備されていなくては安全性は保証されない。安全教育すべきは，むしろ大学の教官ではないかという意見も多かった。その後世論の後押しもあって，実験室はかなり改善されたといわれるが，将来この分野の専門教育を行う人達にきちんと安全と環境保全の教育を行うべきである。

2.4 消費者教育

化学物質を含む家庭用品は，生活に便利であり，また快適さを与えるために利用されているが，これらは危険性をも併せてもつということを，よく認識しておく必要がある。したがって，化学物質による恩恵を最大限に利用し，リスクを最小限度とするための教育が必要となる。

この教育は，本来学校教育において義務教育あるいはそれ以前の段階から計画的に行うべきものであり，化学物質の性質，危険性，使用による人体や環境への影響について自らが主体的に判断できることが望ましい。現在，化学物質に対する見方や考え方を深める基礎的な学習は，学校教育の理科を中心とした教科で行われ，消費者教育は生活科，社会科，家庭科，技術・家庭科を中心に取り組まれている。実生活に結び付いた安全教育や上に述べた防災教育を，これらの教科の間で連携をとって，実施すべきである。そのためには，カリキュラムの総合化，指導者の育成やテキストの作成などに取り組むべきである。

しかし，現状では学校での教育は十分でないので，消費者教育が必要になってくる。ここでは消費者として，いかに安全に生きるかを学ぶべきである。自らが情報を収集，活用し，被害を防ぐのみでなく，家庭用品を最大限有効に利用する技術を身につけるべきである。具体的には，消費者教育用テキストや指導者用資料の作成，指導者育成制度の整備が必要になる。また，一般の消費者が危険性のある化学物質や，その他の事象について，正しい理解を持つことは，社会の不安を防止することに有効である。

2.5 今後の安全教育のあり方と社会

日本はこれまで終身雇用制の国であり，日本人は一旦会社に就職すれば，生涯そこで働くのが常であった。教育のあり方もそれを基本としているところが多い。そのため，オペレータを完全に一人前にするのに 10 年の歳月をかけることも可能であった。しかし，社会は変りつつあり，中途入社の者も多くなっている。短時間に即効的に教育を行い，長期間の経験者と同等ないしはそれ以上の能力をもたせることが重要である。また，これからはオペレータも日本人だけではなく，外国人の採用も十分考えられるので，基本的な考え方，習慣，知識のあり方などの差を考慮することが必要である。

これまでの安全教育は，技術的，技能的な面のみ強調されてきたが，法律的な問題や社会科学的な安全のニーズに関する視点も取り入れるべきである。さらに，国際的な視点と，それに基づいた基準化，規格化もまた重要である。

時代は急速に変わりつつあり，便益に対するリスクを各人が負うべき時代になりつつある。個人が，企業がそれぞれの責任においてリスクに対する安全を考え，実行する時代が来てい

る。全ての分野の企業で安全教育が必要であり，学校においても実施する必要がある。しかも絶えず変化しつつある社会の養成に応える形で行わねばならない。安全工学関係者の多くの英知と指導性が要求される。

3. 国際安全工学・科学研究連絡機構

現在，国際安全研究連絡機構設置準備小委員会で表記の機構の設立を目指して準備を重ね，本1997年6月ポルトガルで第2回のフォーラム（IFSES* II）を開催するよう努力中である。安全工学はシンポジウムが6学会プラス日本人間工学会によって運営されていることでもわかるように，広い分野にわたっており，まさに研究連絡委員会の名にふさわしい機能が要求されている。それを国内だけでなく，海外にも広めようとしているわけである。

もう一つの面は国際基準の問題がある。最近ISOなどの国際基準の整備が進んで来ており，ISO* 9000とか14000とか，国際商取引の前提として，品質管理などの条件を満たしていることが条件となりつつある。ISOはヨーロッパ，アメリカは国内法の世界的拡大という異なった立場で進みつつあり，日本などはその峡間におかれている状況にある。過去2〜3回の安全工学シンポジウムの主要話題の一つである。これの一つの解決法として上述の国際的な研究連絡機構の設置により，積極的に解決することが必要である。

4. 安全工学の社会における位置付けと日本学術会議の今後の活動方向

当初に述べたように，今後の安全工学は，個人の問題のみならず，社会の単位で捉えて，社会のリスクを低減するよう努力することが重要である。これを実現するため

1) 国際連絡機構の創設，できれば日本国内に事務局を設ける。

2) システム工学的な安全工学の確立，とくに古典的安全と数学的基礎を踏まえた安全の融合を図る。

3) 国際基準の組織化と，国内の規制緩和を踏まえて，安全工学に関する法規制の最適化の検討を行う。

4) 産業，研究機関，大学教育の場などにおける，共通の安全工学教育法（カリキュラム，テキストを含む）を検討し，大要を明確にする。

5) 各分野のデータ・バンクを有効活用するための補助手段の原理の検討と具体的な開発を，とくに事故などの過程，社会的重大性，関連因子の認識と，それらの計画，設計への反映・有効活用，を主眼として行う。

などが考えられる。この方向にむけ，日本学術会議安全工学研究連絡委員会は，その主要目標であるいわゆる「パラダイムの変換」について，その線に沿って動いて来た。定常的な安全工学シンポジュウムの開催，1年半に1回程度の安全工学ワークショップ（これは公開シンポジュウムに準じた性格をもたした準公開のもの）の開催，4年に1回の構造物安全性信頼性国内シンポジュウムの開催，これは当初単独，2回め以降は構造工学研究連絡委員会と共催，4年に1回の同内容の国際シンポジュウムの後援など，公開的色彩の強い諸行事を行ってきた。日本学術会議としても，また行政全体としても，このような方向に進むことが望まれる。

結言

安全工学は一見したところ，いわゆる最先端技術ではないが，実際は技術・社会の進展に応じ，つねに変って行くものでなくてはならない。そのため，工学の各分野が独立で行うのではなく，一つの統一した原理・方法・教育などを各分野全体につき統合したものを見出していくことが重要である。本報告の具体的各論を見るとき，社会の安全・安定化について，社会全体の動きと具体的な工学の対象となるシステムと相似性が強いことを念頭に置いて考えるべきであることが理解される。社会全体をシステムと見るとき，各々の装置，システムの安全化は，とりもなおさず社会のリスクの軽減に役立つと同時に，社会システム自体に，その考え方を適用できることがわかる。ここに本報告で提言する4項目の意味がある

最近の多くの事故は，分野が余りにも細分化され，他分野の内容などを理解せず，それぞれ独立に計画などが行われていることによることが多い。システムの計画，設計に当たって，事故などの発生過程のシナリオを各分野にわたって総合的に検討，設定することが不可欠である。

また，社会の安寧のためにも，工学が社会に与える不安を除去し，安心してその利益を享受できるようにすることが大切であり，それを裏付けるためには，法制度の整備などについても工学者は関心を持たなければならない。また，それとともに行政面からも，それを念頭において対処されることが望まれる。

［付　記］

この報告は、第１５期から継続して審議してきたものを取りまとめたものである。

第１５期　安全工学研究連絡委員会

委員長	上原　陽一	(横浜国立大学工学部教授)
幹　事	柴田　碧	(横浜国立大学工学部教授)
	田村　昌三	(東京大学工学部教授)
委　員	板垣　浩	(横浜国立大学工学部教授)
	井上　鉱一	(京都大学工学部教授)
	大音　透	(いわき明星大学理工学部教授)
	大久保　尭夫	(日本大学生産工学部教授)
	小林　英男	(東京工業大学工学部教授)
	斎藤　光	(千葉大学工学部教授)
	杉本　旭	(労働省産業安全研究所主任研究官)
	平野　敏右	(東京大学工学部教授)
	前　郁夫	(社団法人 日本クレーン協会常務理事)

【所属・職名は発足時のものである。】

また、作成に当たって、下記の方のご協力を得た。ここに感謝する次第である。

向殿　政男　(明治大学理工学部教授)

用語解説（*印）

p. 5　IEC: International Electrotechnical Commision（国際電気標準会議）の略. 1908年設立の国際機関，ISO(後述）とともに中心的な役割を果たしている。

p. 10　ハインリッヒの法則：安全問題で事故となること 1 件につき，29 件の小事故と 500 件の過誤的行動があるとする，労働災害で Heinrich によりいわれ出した数値比（潜在的事故についての）。

p. 11　オペラビリティ・スタディ（Operability Study）:操作性研究，一般にはプラントなどの操作性についていう。

p. 11　FTA: Fault Tree Analysis （事故樹），システムでその構成要素が故障をしたとき全体の機能が停止する確率を求める（倒立した）樹枝状のダイヤグラムを使った解析手法

p. 11　ETA: Event Tree Analysis （事件樹），構成原因，要素を追って，それぞれが正常か異常かを樹枝状に最終状態にまで展開して行き，システム全体が異常となるか正常であるかを判定するダイヤグラム，FTA と併用されることが多い。

p. 13　IFSES: International Forum for Safety Engineering and Science, 安全工学研究連絡委員会が海外によびかけ開催している国際安全工学・科学研究連絡機構を設立することについての話し合いのための国際会議，第１回東京，第２回リスボン（本年６月）。

p. 13　ISO: International Organization for Standardization （国際標準化機構）の略 1947 年設立の国際機関，IEC（電気・電子）の分野以外の分野の標準化を行っている。