安全の設計原則と管理

安全技術の発展と技術課題

加部　隆史　（NPO 安全工学研究所）

世の中に存在する動力源を有する製品は凡そ危険なもので安全なものではない。問題は、その「危険」をどのように扱うかである。安全は、人と機械などの危険源の接触から発生する危険事象から人を守る為で、設計の一般原則に基づき世界中の人達が力を合わせ形式知としての規格として作り上げた普遍性を有する。機械技術は多大なる利便性をもたらしたが、幾多の尊い人命の上に成立している。事故が起き、安全規制の見直し及び幾多の方法論の開発という歴史が確認される。安全は人の生命や健康を保護する為有史以来人類にとって尊大であり、現在基本的人権の重要な構成要素となる。安全を暗黙知のみで処理するには限界があり、人類の英知の結集である普遍性を持った形式知で達成される。又、技術面では危険の処理上限界があるため、人と管理に依存せざるを得ない面もあるが、それには決まりが存在する。

1. システム安全から機械安全 （歴史的変遷）

1.1. 産業革命後のボイラー事故多発(1910 年代)

18 世紀以降の産業革命は、駆動エネルギが水力から蒸気へと変遷するに伴い産業用ボイラーが多用され、多くの労働災害事故が発生した。ドイツでは 19 世紀末に社会保障制度創設、事故の災害防止方策としてボイラー検査が開始されたのが、例えば現在の TUEV など現在の第三者検査機関の始まりである。アメリカでは、ASME ボイラーコードが 1914 策定に策定され、その後ボイラー事故は激減した。その 1 年前の 1913 年には ASME 倫理綱領が専門家としての技術者が何たるかを世に告知する為に策定された。丁度その頃、機械防護の基礎或いは安全規格に関する文献がアメリカで発表された(1),(2)。 労働災害で被災者となる労働者の権利を守る為に国際労働機構 (ILO) が設立されたのは 1918 年である。

1.2. アメリカでのシステム安全･確率論(1960 年代)

エリクソン(3),(6)によるとアメリカでのシステム安全は、1940 年代の草の根運動に端を発し、1950 年代に弾みがつき、1960 年代に組織形成され今日に至る発展を遂げた。当時航空機等の幾多の事故調査から多くの知見が得られ、システム安全の概念が煮詰められ、1958 年には最初のシステム安全に関する定量的分析手法が紹介された。1960 年にはアメリカ空軍のミサイル部門 (BMD) がシステム安全事務所を設立し、1962 年に最初のシステム安全仕様書を策定した。1964 年に非営利団体のシステム･セーフティ協会 (SSS) が設立された。前身は 1963 年に設立されたエアロスペース･システム･セーフティ協会で、翌年南カリフォルニア大学の航空宇宙産業部でシステム安全に関する修士コースが設立された。1965 年にはワシントン大学とボーイング社がシアトルでシステム安全会議を開催しこの時点でシステム安全の概念は定着し社会的に組織化もされてきた。

現在、システム安全の教書は MIL-STD-882 であり、これはアメリカ国防省の BSD Exhibit 62-41 並びに MIL-S-38130 が発展したものである。BSD Exhibit 62-41 は 1962 年に出版され安全の原理を紹介しているが狭義でミサイルシステムに限定されており、基本設計から取付迄の範囲であった。1963 年に出版されたアメリカ空軍用の MIL-S-38130 には電子システムが追加され、危険源分析の定義づけがなされた。FMEA, FTA 等もこの頃生み出されている。1966 年に MIL-S-38130 は修正され近代化及びレトロフィットの概念や定性的な危険分析 Gross Hazard Study が追加されたと共にマネジメントの責任が強調された。1967 年には MIL-S-38130A が改定され説明責任が強調され、ライフサイクルに亘るマネジメントがシステム･セーフティ･エンジニアリング

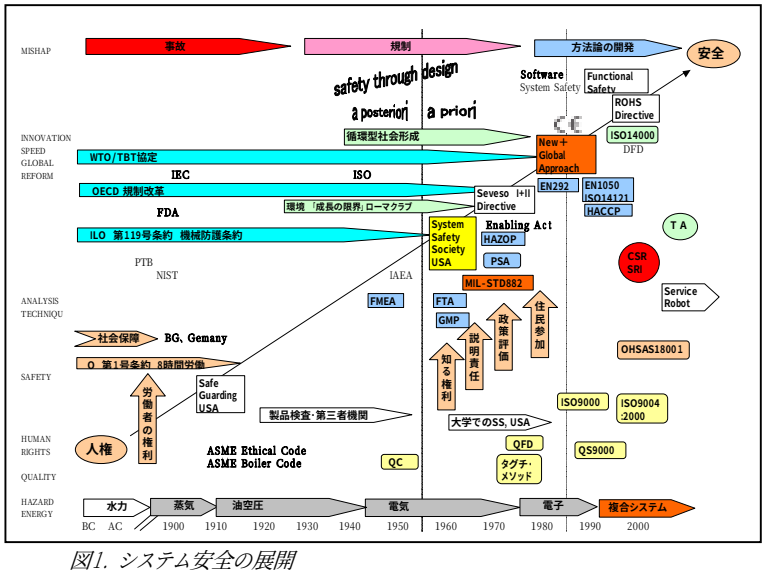

図1. システム安全の展開

プランに言及され契約条項として明記された。1969 年に MIL-STD-882 “System Safety Program for Systems and Associated Subsystems and Equipment”が発行され、全ライフサイクルの概念が導入され、システム安全の要求事項の再構築が求められた。MIL-STD-882A は 1977 年にリリースされ、システム・セーフティ・プログラムにリスク受け入れのコンセプトが導入された。MIL-STD-882B は 1984 年に出版され、ソフトウェアにつき最初に言及された。1993 年に MIL-STD-882C が出版され、主な変更は、ハードウェアとソフトウェアのシステム安全の概念が導入された事である。1990 年大半ばに国防省は規制改革の対象となり、その影響を受けて 2000 年に MIL-STD-882D が発行された。システム要求を実践するプログラム・マネージャーが制定され、軍事要求事項は最小限に限定された。現在 MIL-STD-882E が 2005 年 1 月にドラフトとして提出されている。

アメリカのシステム安全は、航空機・ミサイル産業が主な出発点であり、その後原子力も大いに関連してきたが、科学的方法論（FMEA：IEC60812, FTA：IEC61025, CCF: Common Cause Failure Analysis 等いずれもアメリカの軍用、航空機用、原子力用に考案された方法論）を用いとりわけ信頼性を向上し安全を達成しようとする確率論による「止まらない安全」(4)であり管理手法も導入された。

1.3. 欧州での機械安全・確定論（1980 年代）

欧州では1980年代半ばにニュー・アプローチ及びグローバル・アプローチ関連指令が発令され、安全な製品のみを市場に流通するCEマーキング制度及び基準認証制度の整備と運用上必要な安全に関する設計の一般原則EN292やリスクアセスメントを初めとする機械安全に関する階層的規格構造と**確定論的アプローチ**により、事故の要因となる危険源をどうするから出発し、危険があれば機械を止める（停止の原則）或いは防護する（隔離の原則）事により安全の実現を目指した。日本では杉本・蓬原によるユネイトな情報伝達に基づく確定的な「安全の原理」（4）が基本的に駆動源を有する全機械に適用されると共に一般設計原則の考え方と同一線上に有る「安全確認型」或いは「止まる安全」並びに緊急時の「止める安全」の考え方等が発表された（5）。同時期、WTO/TBT 協定は技術基準につき、個別規定ではなく性能規定を提唱した。主な流れは図１を参照。

1.4. 不確定時代（現在）確定論＋確率論

欧州での CE マーキング制度が発足し 10 年近く経過し、その間システム安全による信頼性・機械の防護に頼った安全確保をしてきたアメリカは欧州の確定論的アプローチを ANSI 規格として採用した。1990年後半になり、確率論に基づくソフトウェアの安全性に関する機能安全規格IEC61508が発行され、停止に関する安全関連信号もソフトウェア処理する事が規格上容認された。主な方法論としては設計と検証に関する V モデル、FMEA,解析手法として CCF:Common Cause Failure Analysis（CCFA）、マルコフモデル、ペトリネット等(6)があげられ、これらの確率的手法は機能安全規格 IEC61508 の構築上必要不可欠となっている。

更には人と機械の協働作業の増加に伴う新たな人の存在検知・存在認識、新たな機械の停止方法等が望まれ、安全関連信号をソフトウェアに頼る場合、機能安全規格が適用される為、確定論＋確率論の集合体となる。そして、機能安全についてはより一層の製品のライフサイクル管理が求められ、規格上でも品質管理ISO9000を基盤とするマネジメントが要求される。これらの要素を踏まえた問題解決として安全技術の更なる進化がなされる。

2. 安全の原則

2.1. 災害防止、止まらない安全から止まる安全

災害防止については1929年の確率によるハインリッヒのドミノ理論（7）からの職場の安全確保、システム安全による科学的・包括的な確率的アプローチとしての止まらない安全、確定的な機械の危険源に着目した止まる安全、緊急時の止める安全とある中で、一貫して安全は人を危険な機械の動きから守る点に着目されてきた。

2.2. 演繹的予防概念の安全設計

安全な設計の為の一般設計原則 ISO12100 は、機械に存在する周知の確定的危険源のリスクアセスメント・リスク低減を定めた方法論であり、同時にア・プリオリな事故の予見可能性並びに結果回避可能性を示す。その意味からも、演繹的予防概念と言える。経済産業省の委託調査(8)によると、機械関連事故のおよそ 8 割は一般設計原則の適用により予見・回避可能である為、その有効性がおよそ 1400 件の労働災害事例をデーターベース構築の上検証した結果により判明している。

2.3. 安全設計原則の適用

現存する各種安全デバイスを中心として一般設計原則を適適用し、実際の作業現場を想定し、適用可能性を検証した所、表1の通り、設備設計時点では最高の安全技術を適用し、人

が介入するシステムにおいては管理(2.7 のマネジメントの意味)に頼らざるを得ない場面が発生する。表1は、危険な機械に人が接近して発生する危険事象を、現在する各種安全デバイスを使用し、人の危険源への複数の接近状態とインターロックを用い、実際の作業現場を想定し、適用可能性を検証した。危険な機械に人が接近して発生する危険事象を、現在する各種安全デバイスを用い、人の危険源への複数の接近状態とインターロック装置による許容条件の組合により、

○＝許容可能、X＝許容不可の他に、△＝中間状態を規定し、定量的評価を行なった。安全の原理(4)では、不確かな状態を危険状態と定義したが、実際には技術的に確定しても 2.5.項に示すように故意に機械の安全装置を人が無効化する状況が特に経済性の観点から発生しうる為、敢えて△＝中間状態を規定した。この定量的評価は、現存する安全技術を全て包括しする訳ではなく、人の危険場所への侵入を複数でなく、1名と限定する為、現段階ではあくまでも参考であり、客観的な総体データには至っていない。設備設計時点では最高の安全技術を適用しても、人が介入するシステムにおいては管理(2.7 のマネジメントの意味)に頼らざるを得ない場面が発生する。

表1. 安全システムの安全性評価

2.4. 安全設計原則と非定常時運転

産業安全研究所の報告によると⑼、非定常時運転を危険点近接作業とし、大方の事故は自動運転中ではなく、人が介在する非定常時運転で発生し、機械設備による死亡労働災害約130件を分析した結果、少なくとも3割以上は危険点近接作業による。その為、安全技術を補完する意味での支援防護装置等の必要性も大いに検討されるべきであると同時に、一般設計原則の適用限界を示している。

2.5. 安全設計原則とドイツでの安全装置無効化実態調査

更に、安全に関する社会システムが歴史的に確立されてきたドイツでは、機械の安全装置の無効化が全体の 3 割程の割合で発生している事が 2 年間に亘る専門家の調査により明らかとなった(10)。無効化の実態は定常時ではなく、故障時等の非定常時作業時が多かった。これが元で事故が発生した際には容認事業者には罰則規定が適用されるのを周知の上で無効化は実施されている。最大の要因は、速度（製造企業にとっての経済性の観点からの生産性）であった。

2.6. 不確定な危険要素 UDF

2.3 から 2.5 の考察は、現在の安全原則の技術面での限界を示し、同時にある程度後述する管理で補う必要性を明示する。しかしながら、現存する有効な科学的方法論並びに安全設計

原則に基づく既存の安全技術は第一義的に充分に適用すべきであり、更にその技術を進化させる必要がある。ここで言う管理とは、設計者が誠実に最高の現存する技術を使用する前提があり、管理側でそれを無効化・改善、不正を働く事を除外し、正当な管理（仕事内容の妥当性の検証）を意味する。それにも係わらず事故が発生する為、これらの現象を総じて不確定な危険要素（Undefined factor :UDF）と呼び、その解決方法は今後の検討課題である。

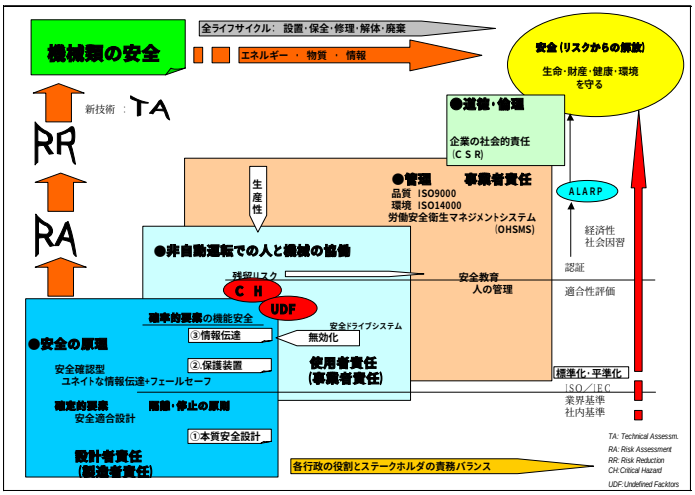

図2. UDF の発生

2.7. リスクマネジメント（管理）

危険源の処理を機械製造者（設計者）が科学及び技術の知見を基に、その時代に可能な最高技術として仕上げ、それ以上の代替設計も理論的には可能であるが実質的に使用者への利便性が損なわれるため、実現可能性に基づき、それを最高技術として、リスク低減に到る危険源の処理方法を既知のリスクアセスメントとリスク低減等の方法論を用い文書化し、その結果残ったリスクについては社会的に受入れ可能とし、使用者へ残留リスクとしての危険源の対処を明文化し委託するという手順を踏み、危険源の管理が設計者（製造者）から使用者への管理へと移管される。その際に、時間軸としては危険源の移管が発生する機械の流通時のみならず、機械の全ライフサイクルに亘る管理と理解する必要がある。設計者はリスクアセスメントとリスク低減の結果ををを第三者機関によりその妥当性を確認する事は説明責任を果たす意味で有効である。

2.3 項での管理とは、ISO/IEC Guide73：2003 に基づくリスクマネジメントの概念に基づき、事業者が行なうリスクアセスメント・リスクコントロール・リスクコミュニケーションの一貫した流れを包括した管理を意味する。マネジメントシステムとしては、品質に関する ISO9000 ファミリー、環境に関する ISO14000，労働安全衛生についての OHSAS18100，CSR に関する ISO26000、情報セキュリティに関する ISO27001 食品に関する ISO22000、プロジェクトマネジメントに関する ISO10006 等が存在し、1990 年代から急速に整備されている。

事故が起きても、直ぐに管理（人）責任を追及するのではなく、確定的な危険源が設計者により適切に処理され、残留リスクの使用者への伝達が正しく行なわれたかを問うのが、本来の姿である。2.1－2.7.の事象の関係を図2に示す。これらの相関関係と特に 2.5 への解決案と 2.7 の相関関係の提示により、今後 UDF の概念がより明確になり、問題解決の必要性が明確化並びに最適化される必要がある。

3. まとめ

機械に関する安全は作業者を守る観点から、人権に端を発し、第一期の 1910 年代産業革命以降の事故増加をそれに対する様々な安全方策、第二期 1960 年代のアメリカに於けるシステム安全概念の育成、第三期 1980 年代の欧州機械指令に見る機械安全概念の成立を経て現在第四期の人と機械の協働の時期を迎えている。事故発生と技術解決の方法論の発展段階を考察し、現在人と機械が共存する段階で発生する不確定要素 UDF を検証・確認し、現状の安全技術の限界から設計の一般原則に基づき処理された危険源（残留リスク）を設計者から使用者へ管理を移管する手順と必要性を明確にした。

参考文献：

(1)Blake, R. Industrial Safety: Fundamentals of Machine Guarding. New York: Prentice-Hall, 1914.

(2)Hansen, C. Universal Safety Standards. 2nd ed. New York: Universal Safety Standards Publishing Co., 1914.

(3) A Short History of System Safety, Clifton A.Ericson、Journal of System Safety Vol.42,No.6, Nov-Dec 2006

(4) 杉本旭・蓬原弘一、安全の原理、日本機会学会論文集第 530 号 C 編、1990

(5) 機械にまかせる安全確認型システム、杉本旭、中央労働災害防止協会、2003

(6)Hazard Analysis Techniques for System Safety, C.A.EricsonII, A Willey & Sons, Inc.,Publication, 2005

(7)ハインリッヒ産業災害防止論、井上威恭監修、海文堂出版 1982 年

(8) 機械安全技術の普及促進事業報告書（経済産業省平成 17 年度高度技術集約型産業研究開発調査）、NPO 安全工学研究所,2006

(9) 危険点近接作業を対象とした支援防護装置に関する基礎的研究、清水尚憲、梅崎重夫、小林茂信、第 34 回安全工学シンポジウム講演予稿集 P153-156,2004

(10) 安全装置の無効化に関する調査報告書;Manipulation von Schutzeinrichtungen an Maschinen, HVBG-2006, ISBN: 3-88383-698-2