解説/Review:

本質安全と確率論的安全評価について

中村 英夫[*1] ・山本 正宣[*2]

Difference Between Inherent Safety and Probabilistic Safety Assessment

Hideo NAKAMURA[*1] and Masanori YAMAMOTO[*2]

Abstract– There are some safety assessment, some of them are inherent safety and probabilistic safety assessment. But, it has not clearly defined of them. This paper reports the difference of both safeties and the way of realizing optimization of Life Cycle Cost of Safety Related System. And it proposes the concept of Safety Cost and reports it on the Railway transmission systems. About the railway systems, the cost loss is fewer than the more safety transportation facilities in signaling systems. So it is important to identify the concepts of the inherent safety and the Safety Cost must need to validate it by the Risk Assessment.

Keywords– inherent safety, probabilistic safety assessment, transportation system, safety cost, risk assessment

1. はじめに

安全に関連するシステム（以下「安全関連システム」）は，その機能として安全が重要であるにもかかわらず，システムを実現する上での経済性の問題などから，充分な安全性が確保されないままに，社会に組み入れられることが多く，事故が起きて社会的に大きな問題を起こしてから，非難される例が多い．その端的な例が東日本大震災の際発生した原子力発電の事故である．既に明らかになっていることであるが，国会などの審議の中で，今回の津波による事故を想定し，対策を取るべきとの主張があった．その主張に対し，極端に確率の小さなことまで想定し，巨額の対策費を投じることは，利用者に過大な負担を求めることになるので取るべきではないという答弁があった．結果的に，そのような東電首脳部の無責任な態度が今回の事態を引き起こしたことは言うまでもなく，非難されるべきである．ただ，本論文においては，そのような批判ではなく，むしろ，その後識者によってなされている議論が必ずしも十分ではなく，このまま推移すると本質を見失うおそれがあるという懸念について主張したいと考えている．

[*1] 日本大学理工学部電子情報工学科 千葉県船橋市習志野台 7-24-1
[*2] （株）シグナルコンサルタント 大阪市天王寺区南河堀町 3-34
[*1] Nihon University, 7-24-1 Narashinodai, Funabashi-shi, Chiba
[*2] Signal Consultant Co. Ltd., 3-34 Minamikawahorichou, Tennouji-ku Osaka-shi
Received: 12 July 2011, 15 August 2011

システムに安全性を織り込む方法としてフェイルセーフに代表される本質安全の立場（本質安全については危険源そのものを取り去ることをいうのだとする狭義の見解があるが，ここでは，フェイルセーフによる対策を含めた広義の立場を取る）と，対策を重層的に施し発生確率を許容レベル以下に小さくすることでよしとする確率論的安全性評価（PSA：Probabilistic Safety Assessment）の立場がある．原子炉は PSA の立場を重視して設計されてきたものであるが，本質安全の立場を最後まで追求することなしに，PSA でよしとしたところに今回の根本的問題がある．

事故後の識者による指摘には，「予備電源を高台に配置すべきであった」とか，「バッテリーを地下に配置したことが誤り」といった類のものが大半であった．しかし，本質安全論の立場に立てば，そもそも電気エネルギを供給し続けなければ，安全が確保されないという仕組みそのものが重大な誤りということになる．

このことは第 2 章で詳細に論述するが，鉄道でいえば，非常ブレーキに用いられる車両の空気ブレーキは，コンプレッサで十分空気を貯め加圧しているときにブレーキが解放され，空気が抜けると自動的にブレーキがかかる．したがって，コンプレッサの故障や空気溜の漏れ，配管の破損といった障害時には全てブレーキがかかる．これに対し，電源の供給が絶たれたことで致命的なモードに移行する福島原発の安全の仕組みは，本質安全論者から見れば，理解出来ない．エネルギが絶たれる

と自動的にブレーキがかかり，安全側に作動するのは本質安全の基本である．また，本論文では，「本質安全などの高度な安全設備を導入するとコストがかさむ」という『常識』について実システムの解析例にて考察する．コスト増という議論は主として製品コスト，システム導入時のコストで論じられる．しかし，実システムで問題になるのは，運用効果や保全，廃棄まで含めたコストすなわち LCC (Life Cycle Cost) である [1]．本論では，比較的安全設備が明確に区分されている鉄道交通を例に，運転事故と輸送障害及び安全投資比率と修繕費比率の関連を評価する．鉄道システムの事例で考察した結果では，安全性の高い設備でシステムを構築した場合，事故発生件数も少なく，収益に対する安全投資額と固定費に対する修繕費の比率も少ないことから，LCC は安価になることが判明した．リスクアセスメント（RA：Risk Assessment）の実施による本質安全設計と PSA による安全設計を LCC で正当に評価すべきと考える．さらに，PSA のもつ本質的危険性についても主張する．

2. 本質安全と確率論的安全について

2011 年 3 月 11 日に発生した東日本大震災では多くの犠牲者と被災者がでました．心よりお悔やみとお見舞いを申し上げます．

災害は，忘れたころまたやって来る．今回の被害の状況を 10^3 年の時系列的に，表面だけでなく立体的に，また学問分野の全体にまたがって多彩な分野の観点から評価し，復興に役立てることが重要と考える．

信頼性は確率によって信頼度として表現され，安全性と深い関係にあるが，異なった概念である．システムは，どんなに高信頼化しても故障は避けられない．よって，安全関連システムは予期しない事象が発生しても，システムを安全な状態に保つ対策を施しておく必要がある．

この意味で今回の福島第一原子力発電所の異常事態は疑問である．「発電用軽水型原子炉施設に関する安全設計審査指針」によると，「自然現象に対する設計上の考慮」に，地震によって機能の喪失を起こした場合，適切と考えられる設計用地震力に十分耐えられる設計であることの他に，「安全機能を有する構築物，系統及び機器は，地震以外の想定される自然現象によって原子炉施設の安全性が損なわれない設計であること」と記されている．「安全機能」とは，「原子炉施設の安全性を確保するために必要な構築物，系統又は機器の有する機能で，原子炉施設の異常状態において，この拡大を防止し，又はこれを速やかに収束せしめ，もって一般公衆ないし従事者に及ぼすおそれのある過度の放射線被ばくを防止し，又は緩和するもの」としている．しかし今回の事故の報道を検討すると安全機能の多くが多重防護の設計に基づいていて，監視機能やその結果の処理は，「危険を検出した場合に安全機能を働かせる」危険検出型である [2–4]．

「安全が確認できているときに限り通常運転を許可する」安全確認型 [5] ではないために本質安全となっていない．危険検出型と安全確認型には大きな相違があることを認識せねばならない．また，PSA は，確かにリスクアセスメントに基づいて RISK を評価しているが，発生確率と被害規模の数値的根拠が確定できない場合の対応が不明確である．さらに，PSA は，重層的に対策を付加していくことにより，理論上はいくらでも RISK を低減できる．そして，その値が受け入れ RISK 水準以下まで低減できると，一件落着として次の危険因子への対応へと視点が移る．しかし，今回のように前提が破綻したときには PSA のみでは無力だ．

PSA を絶対視すると，本質安全による「最後の手段」への思考が及ばぬまま，数値のみで問題なしとしてしまうことがある．津波によって，重層的安全対策がいっぺんに破綻しないかという議論は，国会の場でも行なわれていたという．想定外という言葉を何回も耳にした．確かに我々は神の領域には入り込めない．ただ，神ならずとも危険性を指摘していた人間の声すら無視した背景に，PSA への盲信が無かったか大いに気になる．安易に PSA を持ち出し，本質的議論を回避するのではなく，本質安全設計が何よりも重要であることを謳うべきである．

原子力発電における本質安全について述べる．

原子力発電の安全を本質安全の概念で構築する場合は，最初に安全性要求事項を明確にすべきである．次に，例えば何も制御しない状態では自然界の力で原子炉冷却あるいは停止が継続していて安全な状態が保たれ維持されている構造となっていなければならない．実は，この構造にすることが重要かつ困難なことであることは理解できる．しかし，ここで妥協してはならない．まず，無制御状態がもたらす安全な状態から，エネルギを加えることで冷却あるいは停止を減じて，「通常運転」に移行させる．運転状態においては，所定の数値が制限内であることを常にフェイルセーフ回路で監視し，制限から逸脱した異常状態の数値あるいは監視機能の故障は，エネルギを断つことで元の冷却あるいは停止の状態にさせて，安全を保つ本質安全とすべきである．

即ち，原子炉は何ら外部エネルギに頼ることなく常に安全な冷却状態が保障できていなければならない．例えば反応炉を海抜以下に設置し常時海水で冷却ができる状態にするといったことを意味する．その上で，運転時は原子炉周辺からの冷却水が大量に流れ込むことを「敢えてエネルギを以て」適切な流量に押さえ込む．この状態を常に監視し，一定の稼働率を保障するように「制御」する．ここでいう本質安全とは，安全な状態にシステム

を固定しておき，稼動時は外部から「エネルギ」を加えることで固定以外の稼動状態にし，「エネルギ」の喪失や監視系の故障の際は，外部からのエネルギによる「制御」が消滅して安全状態に自動遷移する仕組みをいう．

3. 安全関連システムの安全コストについて

システム安全の概念は，システムのLC (Life cycle) の要求分析と定義，構想，設計，製造，設置，運用，保全，廃却に亘り，そのプロセスで所定の活動が終了するまで続けられる安全解析や危険源の制御をする活動である [6]．安全関連システムにおいて，本質安全を達成することは多くの費用を必要として社会的に受入れ可能なコストを実現することが困難であると言われる事例が多い．原子力発電もこの範疇の議論がなされ，PSAで安全が達成されているのに，安全対策を強化し余計なコストを掛けることは利用者に過度の負担を強いることになり容認できないという詭弁がまかりとおっていた．PSAの数字が，本質安全への挑戦を回避させ，潜在的危険側の芽を残したままにするとしたら，問題は大きい．ところで，議論の際に用いられる「経済性」であるが，システムのLCを通しての総合費用を比較すると，例えばPSAで構築したシステムの方が本質安全で構築した場合より経済的であるとは限らない．

まず，筆者らが提案する安全を構築するための費用である安全コストの概念は，「安全関連システムの構築に際して，そのシステムのLCにわたって必要とする安全を確保するために必要な総コスト」と考える．

一例として，鉄道交通の規格である，IEC62278：Railway applications-Specification and demonstration of reliability, availability, maintainability, and safety (RAMS) では，次に示す作業を安全に関する作業としている [7]．よって，これらの作業に伴うコストを安全コストとしてシステムの経済性の比較の際に用いるべきである．

(1) 概念: プロジェクトの安全上の意味の考慮及び安全方針と安全目標の見直
(2) システム定義と適用条件: 過去の安全の経験データの評価，予備危険源分析の実施，安全計画の確立及び既存設備などの制約条件の安全への影響の特定
(3) 危険分析: システム危険源と安全危険分析の実施，危険源日誌の設定及び危険評価の実施
(4) システム要求事項: システム安全要求事項，安全受入基準，機能要求事項の規定及び安全管理の確立
(5) システム要求事項の割当: システム安全目標と要求事項の割当，サブシステム・コンポーネントの安全要求事項の指定と受入基準の規定
(6) 設計と実施: 見直し，分析，試験及びデータ評価による安全計画書の実施，危険源日誌，危険源分析と危険評価，安全関係設計決定の正当化，プログラム制御の実施，安全管理，下請業者と供給者の管理
(7) 製造: 見直し，分析，試験及びデータ評価による安全計画の実施，危険源日誌の使用
(8) 設置: 設置プログラムの確立と実施
(9) システム検定（安全受入と立上を含む）: 立上プログラムの確立と実施，用途固有の安全事例の作成
(10) システム受入: 用途固有の安全事例の評価
(11) 運転と保守: 継続的安全関連保守の実施，継続的安全性能監視と危険源日誌の保守の実施，事故対応
(12) 性能監視: 性能と安全統計の収集，分析，評価，使用
(13) 改造と後付: 改造と後付の安全上の意味の考慮
(14) 使用停止と処分: 安全計画の確立，危険源分析と危険評価及び安全計画の実施，環境アセッスメント

安全関連システムの安全コストは，内容的に確立しているわけではないが，システム安全を構築するために必要不可欠な事項としての認識を持ち，安全コストを明確化して，より安全性を高める意思決定が，LCCを考慮した場合，結果的に非常に有効であることを認識すべきである [8]．次に，この認識を鉄道システムの具体的な事例で検証する．

4. 鉄道交通の安全関連設備投資

4.1 安全関連設備投資と障害及び事故との関連

安全関連システムは，システム全体としての安全対策が有効であることが，各輸送システムの事故件数，設備投資及び安全関連設備投資の比率に関する評価から得られている [9]．そこで鉄道交通の安全設備の違いによる障害及び事故との関連を評価する．

LCCは，製品の生涯で発生する費用の総額であり，

LCC ＝取得コスト＋所有者コスト＋廃却コスト

所有者コスト＝運転コスト＋保全コスト
＋間接損害コスト　である．

鉄道システムにおいて公表されている費用 [10] をこれらに適用する場合，次の区分とした．

取得コスト＝開発・設計コスト＋製造・設置コスト
＝鉄道事業固定資産

所有者コスト＋廃却コスト
＝鉄道事業設備投資＋施設・車両の修繕費
＋安全関連設備投資
＝設備投資

なお，評価は，年度ごとの合計費用を総コストとした．さらに，鉄道交通の安全関連設備投資の内容は，安全に関係する機器の設備投資が主であり，システム全体の安全に関する安全コストが含まれているわけではない．

平成18年度から21年度ごとの各鉄道事業者区分による総コストを求め，この値と鉄道事業固定資産，設備投

Table 1: By demarcate of the railway enterprise on the division of cost and the number of railway accidents and troubles

鉄道事業区分/年度		① (%)	③ (%)	⑤ (%)	⑥ (%)	⑦ (百万円)	⑧ (百万円/km)	⑨ (百万$^{キ_{ロ}}$)	⑩ (百万$キ_{ロ}$)	⑪ ATS(%)	⑪ ATC(%)
JR 在来線/JR 新幹線	H18	34.0	3.16(9.28)	13.4	86.6	12,790,322	638.93	0.60/0.01	1.85/0.17	99.0/0	0.98/100
	H19	40.0	3.59(10.5)	14.6	85.4	12,901,246	645.1	0.62/0.01	1.67/0.13	98.6/0	1.43/100
	H20	34.0	3.4(10.8)	14.1	85.9	12,795,884	640.15	0.60/0.01	1.45/0.19	98.6/0	1.43/100
	H21	31.9	3.5(10.9)	14.3	85.7	12,804,402	640.58	0.62/0.01	1.40/0.16	98.6/0	1.4/100
大手民鉄	H18	23.5	2.99(12.7)	10.4	87.3	5,443,320	2,036.5	0.66	0.31	97.3	2.71
	H19	22.8	3.78(15.6)	12.7	87.3	5,686,717	2,131.3	0.70	0.15	96.7	3.3
	H20	23.0	3.46(15.0)	11.2	88.8	5,607,675	2,100.5	0.65	0.21	96.6	3.4
	H21	22.2	3.45(15.5)	10.9	89.1	5,654,831	2,116.6	0.68	0.18	95.7	4.32
公営地下鉄	H18	11.0	0.85(7.75)	4.52	95.4	7,476,445	10,648	0.47	0.39	2.61	97.4
	H19	11.1	0.92(8.3)	4.22	95.8	7,608,418	10,462	0.41	0.25	2.52	97.4
	H20	13.0	1.21(9.3)	5.30	94.7	6,575,173	8,821	0.46	0.41	0	100
	H21	11.0	1.16(10.5)	4.8	95.2	7,623,142	10,226	0.43	0.27	2.46	97.5
新都市・モノレール	H18	14.6	0.89(6.06)	5.83	94.2	489,069	2,471.3	0.25	1.15	0	100
	H19	15.5	1.23(7.9)	5.66	94.3	483,029	2,440.8	0.15	1.5	0	100
	H20	11.5	2.32(14.0)	8.22	91.8	481,559	2,433.3	0.05	0.53	0	100
	H21	12.8	1.7(13.2)	5.36	94.6	1,723,244	8,837.1	0.05	1.01	3.36	96.6

(注)(1)数値はH18年度からH21年度である．H21年度の新交通・都市モノレールの設備投資額が非常に高いのは，大阪市で新線建設など複数の事業者区分の設備投資実績などを一括して計上したためによる．

(2) ①は，事業収益/総コストの比率．③は，安全関連設備投資/総コストの比率で，( )は安全関連設備投資/事業収益の比率．⑤は，設備投資/総コストの比率．⑥は，固定資産/総コストの比率．⑦は，設備投資と固定費との合計である総コストで単位は百万円．⑧は，総コスト/営業キロ(百万円/km)．⑨は，列車百万キロ走行当たりの運転事故件数．⑩は，列車走行百万キロ走行当たりの部内の輸送障害件数．⑪は信号保安装置の営業キロに対する設備比率である．なお，⑨〜⑪はJRの在来線と新幹線のそれぞれの比率(在来線/新幹線)を示している．

資，安全関連設備投資などの比率を求めた結果を **Table 1** に示す．安全関連設備投資は，総コスト，事業収益のそれぞれの比率を求めた．その結果次のことが判明した．

(1) JR では在来線と新幹線の諸費用の区分が不明なために設備の違いによる LCC の違いが不明確であるが，事故件数及び輸送障害は，ATS（自動列車停止装置: Automatic Train Stop）が主な在来線に比べ ATC（自動列車制御装置: Automatic Train Control）が設備されている新幹線の方が 1 桁以上少ない．

(2) 大手民鉄は，97.3%が ATS を設備している．公営地下鉄と新都市・モノレールは ATC を設備している．

大手民鉄と新都市・モノレールの比較から，

① 安全関連設備投資対総コストの比率は，前者が約 3 倍多い．

② 設備投資対総コストの比率は，前者が約 2 倍多い．

③ 固定費対総コストの比率は，前者が約 2 割弱少ない．

④ 列車百万キロ走行当たりの事故件数は，前者が約 8.5 倍多い．

⑤ 列車百万キロ当たりの輸送障害は，大手民鉄と公営地下鉄でほぼ同じであるが，新都市・モノレールは約 5.5 倍多い．

これら事業者区分による数値の比較評価は，踏切道の有無，安全設備の違いなどがあり一様に比較できないが，傾向は把握できると理解する．

即ち，ATS と ATC で比較した場合，安全性は ATC の方が高く，安全関連設備投資と設備投資の総コストに対する比率は ATS の方が高く，固定費の総コストに対する比率は ATC の方が高い結果となった．よって，ATS は ATC に比べ，取得コストが少ないが，所有者コストは高く事故件数も多い．ATC は取得コストが高いが，所有者コストは安く事故件数も少ないという結果になった．

さらに営業キロ 1 km 当たりの総コストを事業者区分から検討すると，大手民鉄と新都市・モノレールはほぼ同じ額であり，公営地下鉄は他より約 5 倍高い．これは地下鉄の線路建設に多額の費用がかかるためと理解する．しかし，大手民鉄と新都市・モノレールは，地上に設備されているために，2 割後者が高い程度である．ここで，取得コストと所有者コストの総コストに対する比率の違いから年度ごとの総コストを積分して，両者のコストが同一になる年数を Eq. (1) で想定すると，平成 18 年で 6.4 年，平成 19 年で 2.3 年，平成 20 年で 9.4 年であった．

$$\text{大手民鉄の 1 km 当たりの総コスト} \times (1 + n \times ⑤/100) = \text{新都市・モノレールの 1 km 当たりの総コスト} \times (1 + n \times ⑤/100) \quad (1)$$

ただし，⑤は設備投資 / 総コストの鉄道事業区分のそれぞれの年度の比率（**Table 1** 参照），n は年数．

よって，最初から ATC の設備で建設した場合，その後の鉄道事業設備投資，安全関連設備投資と施設・車両の修繕費が ATS より少なくて済み，LCC を考慮すると

ほぼ 10 年以内に ATS 設備より安くなることが想定される．あわせて事故件数も少なくて済む．

鉄道技術者の一般的常識に，優等線に設置される ATC は ATS よりコストが高いという見解がある．しかし，LCC の評価では，必ずしも常識が真理ではないことが導けた．安全関連システムは，構想・設計段階から本質安全でシステム設計をすることが必須であるとすべきである．その際コスト的比較から，PSA による代替案が選択されるとしても，再度 LCC で評価する慎重さが欲しい．

5. まとめ

人命に関わる安全関連システムは，リスクアセスメントを実施し，LC の各段階に亘って本質安全で構築することが重要であることを主張した．この見解を事例で補強し，適切な安全コストを提案できるようにしたい．

課題として，環境問題，事故損失額を LCC 評価の対象として，安全対策の投資費用と事故損失額との相関を解明して，より有効な安全対策を早急に行う必要がある．

参考文献

[1] N. G. Leveson: “SAFEWARE, System Safety and Computer,” ADDISON-WESLEY, pp. 159-161, Sep. 1995.
[2] 連載講座 軽水炉の確率的安全評価（PSA）入門，第 1 回～第 7 回，日本原子力学会誌，Vol.48，No.3，2006～Vol.48，No.10，2006.
[3] 日本原子力学会，原子力安全調査専門委員会技術分析分科会: 福島第一原子力発電事故からの教訓，Sep. 5 2011.
[4] 石川迪夫: 福島第一原子力発電事故対応に向けて，日本原子力技術協会,（2011.04.11）.
[5] 安全技術応用研究会: 国際化時代の機械システム安全技術，日刊工業，pp. 21-50，Apr. 12 2000.
[6] H. E. Roland, B. Moriarty: “System Safety Engineering and Management,” John Willy & Sons, Inc., pp. 8-10, pp. 29-61, 1990.
[7] IEC62278: “Railway applications-Specification and demonstration of reliability, availability, maintainability, and safety (RAMS).”
[8] 山本正宣，中村英夫，夏目武，古野紀雄: 安全コストの考え方，第 22 回秋季シンポジューム，日本信頼性学会，pp. 77-80，Nov. 2009.
[9] 夏目武編著: ライフサイクル コスティング，日科技連，pp. 180-200，July 27 2009.
[10] 国土交通省鉄道局: 鉄軌道輸送の安全にかかわる情報，平成 18 年～平成 21 年，及び資料編.

中村 英夫

1948 年 7 月 12 日生．71 年国鉄・中央鉄道学園大学課程電気卒，86 年東京理科大工学部 2 部電気卒，92 年鉄道総合技術研究所研究室長，94 年日本大学に転職，列車制御システムの開発研究に従事，現在に至る．元信頼性学会会長，電子情報通信学会フェロー，工学博士．

山本 正宣

1966 年山梨大工卒，03 年日本大学大学院理工学研究科博士後期課程修了．日本信号（株）を経て，05 年 2 月（株）シグナルコンサルタント取締役，日本大学理工学部非常勤講師．現在に至る．システム安全の経済的最適化に関する研究に従事．電気学会など，博士（工学），技術士（総合技術監理，電気・電子）．