平成23年7月1日発行

IEEJ Industry Applications Society News Letter

電気学会産業応用部門ニュースレター 2011年7月号 (http://www2.iee.or.jp/ver2/ias/nl/)

「『本質安全にもっと光を』原発の事故に想う」

電気学会 産業応用部門 交通電気鉄道技術委員会委員長
中村 英夫（日本大学）

鉄道の列車制御においては，フェールセーフと称する本質安全設計を旨として安全を確保してきた。装置や機械，そしてシステムに至るものが，人間に何らかの便益を与えようとして産み出されたとするなら，全て安全と無縁ではない。その安全も，装置やシステムに応じ手段や方法論が様々だ。このことが，フェールセーフや本質安全を共通の土俵で論じることの困難さを産み出してきた。

例えば，トンネル火災を除くと，鉄道の安全は，システムを停止させることにより維持される。しかし，交通管制のような制御システムでは，機能をなんとか継続する努力が安全につながる。それぞれの産業分野において，「安全技術」の担い手が活躍している。彼らに共通する事は，対象システムに対する豊富な知識と経験である。安全技術はその上に構築されるが故に，安全技術を共通に論じることを難しくしている。1980年代に学会のシンポジウムで各産業分野におけるフェールセーフ技術が議論された。結局，個別分野の豊富な安全性技術が開陳されたが，分野によりフェールセーフの定義も多様で共通認識には至らなかった。

一方，停止側が安全とされる鉄道や工作機械においては，共通の概念で整理される本質安全設計が見いだせる。光軸式物体検出センサには，物体が光軸を遮断したときに検知するものと，物体からの反射光を検知するタイプの2種類がある。自動ドアなどでは後者のセンサが用いられている。しかし，人間が危険領域にいるか否かの判断に使う場合に反射式は使えない。光ビーム送信部が万一故障していた場合には，人間を検知できないからである。これに対し，前者の遮断型では，構成部品が故障時には，受信入力がなくなるので人間有りとして処理でき，安全である。このように，安全システムの構築においては，エネルギを以て「安全」であることを伝達し，エネルギが届かなくなったときに安全側に遷移させるという共通原理が用いられる。反射型センサはエネルギを用いて危険な状態を伝える方式で「危険検出型」と名付け使用を制限している。

しかし，停止側が必ずしも安全側にならないようなシステムや複雑な故障モードを持つシステムでは，このような原理のみでは対処できない。互いの差への理解が埋めきれず，安全技術に対する不毛な議論も見られた。

このような個別領域に閉じた中での安全技術の検討に代わり，安全を共通の言葉で論じ評価する方法論を与えたのが確率的安全性解析PSA (Probabilistic Safety Analysis)であった。危険因子を致命度と頻度を基にRISKで評価し，RISKの大きいものから対策を立て，許容される水準以下まで低減するという方法論はあらゆる分野に共通に適用できる。

列車制御の分野でも，装置のコンピュータ化が進み，故障モードが複雑になる中で，PSAの方法論は，致命的因子を漏れなく抽出できる方法論として重視された。ただ，鉄道の世界では，本質安全設計を第一とした上でPSAにより安全レベルの確認を行なうという思想がまだ残っている。

今回の福島原子力発電所の事故は，PSAの陥る落とし穴を改めて浮き彫りにした。PSAの考え方に立てば，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，その値が得られるや，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，「最後の手段」への思考が及ばぬままOK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，国会の舞台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。たしかに我々は神の領域には入り込めない。ただ，神ならず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。

ポンプを用いて冷却水を汲み上げ続けるというのは，エネルギ供給を以て安全状態を維持することになる。エネルギが絶たれれば危険側に動作するという機構は，PSAでRISKを低減できても，本質安全の思想からは誤設計として否定される。炉心を海抜以下に配置するならば，エネルギが絶たれても水は供給できる。本質安全設計を最後の手段として真剣に議論することを再確認する必要がある。