マトリックス・ランク法による FA システムの安全性評価法

中田機械技術士事務所
技術士　中田　昭

1. FA システムの安全性評価に関する調査研究の経緯
2. FA システムの安全性評価法
3. マトリックス･ランク法による FA システムの安全性評価法

1．FA システムの安全性評価に関する調査研究の経緯

1980 年代の頃から自動車および電機等の産業界では PLC やコンピュータなどを活用したエレクトロニクス制御によるロボットや自動機械を組込んだいわゆる FA システムの開発導入が盛んに進められるようになりました。それにつれて、従来の生産設備では人的過誤や作業基準不順守などによる事故が殆どでしたが、FA システムにおいてはシステムの信頼性不足に基づく故障や電磁波など外来雑音による誤動作あるいはシステムのブラックボックス化による操作ミスまたは保全ミスなどによる新しい事故が報告され始めました。また、諸外国でも同様の問題が増えはじめてきたことから、ISO でも生産設備の安全に関する規格の制定･見直しが計画されるようになってきました。

そこで通商産業省工業技術院ではこれらの国際規格との整合性を考慮した標準化（JIS 等）の推進を図るため、「FA 標準化推進計画」の一環として「**FA システムの信頼性･安全性の標準化に関する調査研究**」を企画し、（財）国際ロボット･エフ･エー技術センター：IROFA（現製造科学技術センター：MSTC）に委託し、1989 年 4 月から 1994 年 3 月までの 5 ヵ年計画で実施されました。

この調査研究の結果、FA システムの個別要素についての安全性に関する規格･基準は制定されてきているが、包括的な「FA システムの安全性評価方法」が日本国内はもとより国際的にも標準化されたものがないことが判りました。そのため、その成果の一部（「FA システムの評価方法」）をもとに包括的な「FA システムの安全性評価方法」について次のメンバー（カッコ内は当時の勤務先）による「FA システム安全性評価分科会」を編成し、日本工業規格（JIS）へ提案することを目標にして 2 年間にわたり継続調査研究を行いました。

鈴木喜久主査（東京工芸大学教授）、　夏目武（筑波技術短期大学教授）
新家達也（日立製作所生産技術研究所）、　岩谷勝三（オムロンシステム総合研究所）
戸谷清（富士ファコム制御第 1 技術部）、　小田征宏(鹿島建設)
黒須則明（トヨタ自動車 FA システム部）、　中田昭（日揮生産システム開発部）

分科会では、当時の国際的な状況について次の規格などを参考調査して、1996 年 4 月に独自に開発したマトリックス･ランク法を基本にした「FA システムの安全性評価方法通則（案）」を工業技術院に報告しました。しかし、対象となる FA システムが自動車、家電産業のみならず全ての加工組立産業にわたる広範囲になり過ぎたことから日本工業規格（JIS）の対象として審議されるに至りませんでした。

- ISO 1161:Industrial automation systems – Safety of Integrated Manufacturing systems- Basic requirements（1994 年 4 月発行）
- IEC1508:Industrial – process measurement and control（1996 年制定）
- BS 8800:Guide to Occupational health and safety management systems(1996 年 5 月発行)

その後、主査の鈴木教授の熱意によりこの成果は、ISO TC184 に 1998 年 4 月に英文化して“Matrix－Rank method for safety evaluation of integrated manufacturing systems”、また 2001 年 5 月には（社）電子情報通信学会を通して IEC へ TTA-Technology Trend Assessment Document の一つとして“MATRIX-RANK Method for Safety Evaluation of Complex Systems”と題して国際的な規格協会や学会に発表されております。

本日は技術士の諸先生方に御参考になればと考え、1998 年 ISO 向けに発表された「マトリックス･ランク法による FA システムの安全性評価法」の概要を紹介させていただきます。

2．FA システムの安全性評価方法

1）安全性評価の目的と評価手法

FA システムの安全性評価は、**「工場内・外の全ての人に対して生産工場や FA システムがどのように安全であるか否かを包括的に評価する」**ことが重要です。即ち、工場の立地条件、FA システムの生産活動の目的、性能と運転・操作方法などを考慮した「安全衛生対策」、関連設備の「防災対策と公害対策」、要員（管理者および作業者）への「安全教育」および社会的ニーズが高まっている「環境管理」などについて包括的に評価を行い、適切な安全基準と設備および生産活動の安全管理に反映することを目的にした評価手法が必要です。

なお、対象とする FA システムはディスクリートな部品や製品のハンドリングを行う「加工・組立・検査・物流」などの生産システムを対象とし、鉄鋼や化学の連続生産プロセスは含んでいません。

2） ライフサイクルを考慮した安全性評価

FA システムの包括的安全性評価は、システムのライフサイクル毎に適切な評価目的を選択して実施することが重要です。分科会は、表 1「FA システムのライフサイクルを考慮した安全性評価」に示すようにライフサイクルの段階と評価目的を定義し、次の事項を参考にして表3「安全ランク・マトリックス表」の該当項目について評価することを推奨しています。

（1）FA システム全体の基本的安全性（戦略）に関する評価は、次の手順で実施する
- ① 計画・設計・製作・工事段階における「安全設計審査」および「組立工事完了時安全診断」にて事前評価
- ② システムの調整完了後の試運転段階における「試運転時バリデーション」

（2）FA システムの危険（事故）の無害化対策および異常の局所化対策に関する評価は、構成する各機械設備および制御装置について次の検査および評価試験にて実施する
- ① 製作・組立段階における「出荷検査」または「受入検査」
- ② 試運転段階における「試運転時バリデーション」

（3） FA システムが操業・運転段階入った後の安全性評価は、定期的な保守・保全あるいは必要に応じて行う改善・修理作業ごとにその目的や作業内容にあわせて適切な評価項目を選択する

表1． FA システムのライフサイクルを考慮した安全性評価

ライフサイクルの段階		安全性評価目的
計画・設計・製作・工事段階	システム計画段階	システムの安全管理基準（防災体制、公害対策、安全衛生対策、安全教育）を作成し、基本的安全性の評価をする
	システム設計段階	システムの構成要素、除去できないリスク、設備レイアウト、安全防護対策などに関する信頼性・安全性設計基準を作成して、システム設計について「安全設計審査」を実施する
	システム製作・工事段階	メーカーの「出荷検査」または発注者の「受入検査」により、システムの構成要素について安全性の評価を実施する
		システムとして統合した後「組立工事完了時安全診断」として総合的（機械的および電気的）安全性の評価を実施する
試運転段階		システムの「最終安全診断」として、無負荷および負荷試験運転による「試運転時のバリデーション」を実施する
操業・運転段階	通常運転時	システムの日常点検、監視作業をとおして安全教育およびシステムの安全性について再評価を行う
	異常発生時	被災者の救護措置および 2 次災害防止、復旧、原因追及と対策をとおして、事故・災害事例の記録および再評価を行う。 フォルトツリー分析（FTA）にて再発防止対策を検討する
	保守・保全時	機械系および電気系の遮断、危険物の処理、作業の安全防護対策をしながら、保守・保全作業について安全性の評価をする

3．マトリックス･ランク法による FA システムの安全性評価法

ところで、安全性評価方法にはその目的によって表2．に示すように多種多様な手法が開発/採用されています。

表2．代表的な安全性評価手法

評価方法	主な特徴（目的）
1）定性的評価：「チェックリスト法」 「MORT（Management Oversight Risk Tree）」	チェックリストによる安全点検は安全診断の必要条件であるが十分条件ではない
2）定量的評価：「危険度指数評価」 「FMEA(Failure Mode and Effect Analysis)」	危険性の重大性に応じた安全対策を決めるために行う分析手法
3）事故原因のツリー解析：「魚の骨図」 「FTA（Fault Tree Analysis）」 「ETA(Effect Tree Analysis)」	事故の原因分析が定形化されていて明確であり、容易に理解される。 しかし、経験的なデータ少ないヒューマンエラーの評価は難しく、また分析者の判断で評価が影響される。
4）問題発見のための評価 「HAZOP(Hazard and Operability Study)」	「どのような原因からずれ（異常）を生じるかを検討する」方法で事故の発生を想定して安全管理（安全設計など）を行うために用いられる。

しかし、表2.に示す手法は個別の事象や機器の安全性評価には十分ですが、生産工場あるいは FA システム全体の包括的な安全性評価には十分ではありません。そこで、FA システムの包括的な安全性評価法として、表3．に示す縦軸の「安全対策」と横軸の「対象範囲」の 2 次元マトリックスを構成し、個々の評価項目をランク付けする「マトリックス･ランク法」による評価法を考案しました。

表3．　安全ランク･マトリックス表

安全対策＼対象範囲		設計･製作	運転操作	保守･保全	第三者･環境
安全の基本対策（戦略）	職場設計（人間工学応用）	自動化率（省人･省力化）	環境快適性（作業環境）	保守･保全作業回数	遮蔽率（隔離）
	安全管理体制	安全適応性	安全作業管理（訓練教育）	保守･保全管理（訓練教育）	環境管理（公害対策）
	信頼性	システム安全度（安全品質）	停止率（故障率）	作業の安全度（補修頻度）	安全防護
	監視･診断	故障診断性能	検知警報性能	検知警報性能	監視･警報
危険の無害化対策	インターロック	インターロック設置率	インターロック解除率	インターロック設置率	安全設備（侵入防止）
	フェールセーフ	→	フェールセーフの完全性	←	公害対策設備（水、ガス処理）
	フォールトトレランス	→	作業の余裕･多重化率	修復機能	消防設備 防災設備
異常の局所化	非常（異常）対策	非常（異常）停止装置	非常警報 非常停止率	機能部品･装置のモジュール化	非常警報 避難広報
	停電対策	電源の多重化	停電対策	停電対策	—
	災害対策	耐災害レベル	避難体制	避難体制	拡散防止

1） 安全対策

安全対策に関する項目は、表4．に示すように 3 つに大区分し、さらに10項目に中区分しております。なお、中区分は、システムの構成や運転操作の条件等によって適当な項目を選択して追加あるいは置換えして、適切な安全性評価を行うものとします。

表4．安全対策評価項目

大区分	中区分	内容
「安全の基本的対策」[企業の安全基本方針（理念・法令遵守）を反映した戦略的な安全対策に関する評価項目]	職場設計	人間工学を応用した快適な職場設計
	安全管理体制	安全を確保するための管理監理組織
	システムの信頼性	安全を確保する信頼性の高い安全設計
	システムの監視・診断	システム・要素機器を監視・故障診断して異常を早期に発見・表示および修復
「危険の無害化対策」[発生した故障・事故が人に危害を与えないようにするためのシステム機能の安全対策に関する評価項目]	インターロック	ハザードの波及を遮断し、人間と機械の相互干渉を防止するシステム機能
	フェールセーフ	故障や事故を拡大させずに収束させるシステム機能
	フォルトトレランス	システム全体の機能不履行を防ぐ代替システム機能
「異常の局所化対策」[非常・異常時に危険を局所的に抑えて他に影響させない安全対策に関する評価項目]	非常（異常）	異常発生時の緊急安全対策
	停電	突然の停電による人身事故およびシステムの暴走防止機構
	災害	火事、地震、洪水などの対策

2） 対象範囲

FA システムの安全性評価の評価対象範囲を次の4つに区分しております。

（1）「FA システムの設計・製作」：システムの設計・製作の仕様・性能に関する範囲

（2）「FA システムの運転操作」：運転操作要員に対する安全性に係わる範囲

（3）「保守保全作業」（設備管理）：システムの保守保全要員に対する安全性に係わる範囲

（4）「第三者・環境」：工場内・周辺の影響を受ける第三者および地域環境管理に係わる範囲

なお、マトリックス・ランク法による安全性評価を容易に行うには、システムの規模（大きさ）や立地条件（場所）あるいは安全性の評価目的などによって、評価対象範囲を取捨選択します。また、システムを構成する機械設備や制御装置/システム個別の安全性評価は、関連する安全規格・基準と合わせてその使用目的、運転方法に応じて別途単独に評価します。

3） 安全ランク

表3．のマトリック表に示す評価数値は次の表5．の安全ランクにて定義されます。この評価数値の標準的尺度は参照資料（平成 9 年 3 月の報告書）に記載されているので参照してください。

表5．安全ランクの定義

[0] ：経済的に実現可能であり、努力して達成すべき安全レベル	通常安全と考えられるレベル
[+1]：現状において通常達成されていることが多い安全レベル	
[-2]：危険・事故のポテンシャルのない理想的なレベル	マイナスの値が大きい程安全性が高い
[-1]：危険・事故のポテンシャルはあるが理想に近いレベル	
[+2]：改善・対策をした方が良い安全レベル	プラスの値が大きい程安全性が低い
[+3]：改善・対策が必要な安全レベル	

＜参照資料＞

- 「FA システムの信頼性・安全性の標準化に関する調査研究成果報告書」平成 6 年 3 月（財）国際ロボット・エフ・エー技術センター
- 「II.FA システム安全性分科会関係（生産時点情報管理技術（POP）等の標準化に関する調査報告書）」平成 9 年 3 月（社）日本機械工業連合会、（財）製造科学技術センター