システムの安全性分析手法

制御システムの安全性能の検証と妥当性確認に関して、代表的な分析手法及び本研究におけるエレベーターのＦＭＥＡ(故障モード影響解析)試行の概要について記述する。

○代表的な分析手法

制御システムの安全性能の検証と妥当性確認の方法には、分析による方法と試験による方法がある。

試験による妥当性確認は、安全機能について直接試験を実施して要求事項への適合性を実証する方法である。一方、分析による妥当性の確認方法には、演繹的手法により結果から原因をさかのぼって論理的に連鎖メカニズムを遡及する方法と帰納的手法により調査から得られた事実を積み上げて原因から結果へとプロセスを推定する方法がある。

代表的なものを列記すると以下の表のようになる。

表　システムの安全分析手法

手法別	手法名	概要
演繹的手法	FTA (Fault Tree Analysis)	危険事象に対する原因となる事象とその事象に対する防護手段の検討を階層的に実施し、FT を作成する。FT が出来たら FT の構造分析を行い、定量化する。
	ETA (Event Tree Analysis)	まず初期事象を設定し、初期事象からの事故進展を考慮しながら、進展キーの項目を設定する。各進展キーの成功/失敗を統合することにより、シナリオを作成し、最終事象がどのような事象になるかを判断する。その後、定量分析や対策案の抽出といった分析を実施する。
帰納的手法	FMEA(Failure Mode and Effects Analysis)	システムの構成要素から出発してシステム全体に与える影響を調べる解析方法である。
両手法の使い分け	HAZOP 法	設計からのずれの起こる箇所及びその原因と結果を明らかにするために、プロセスの各部を調査することである。
	GO-FLOW 法	システム信頼度、アベイラビリティの評価が行なえる。システムの構成・機能をモデル化するため信号線とオペレータで構成される GO-FLOW チャートを作成し、オペレータの動作モード・故障に対して発生確率をデータとして与え、オペレータ機能の定義に基づき信号を処理してゆき、最終的に系の動作/不動作確率を求めるもの。化学プラント、原子力プラント、交通システムなどの大規模・複雑な動作モードを持つあらゆる種類のシステムの解析に適用できる。

		この方法は、解析過程をほぼ自動化した機器の経年劣化及び保守点検を考慮した確率論的な信頼性解析（経年劣化 PSA）、人間行動と機械の動作を一体として扱う信頼性解析（人間信頼性解析）も可能である。
	FMFEA 法 （Failure Mode Factors and Effects Analysis）	構成部品の故障モードについて、その要因及び影響の解析をそれぞれ FTA,ETA を利用した複合型の安全性評価法である。要因系と結果系の詳細な解析を進めることで、問題の発見と予測ができる。
	S-H 検討法	誤使用に対する安全性の関係をマトリックス図法で解析する方法で、横軸 S が使われ方（Software）、縦軸 H が構成部品（Hardware）であり、マトリクスの枡の中に、発生度、影響度、検知度、総合の評価点を記入する。

分析手法の一つとして GO-FLOW 法が提案されている。　GO-FLOW 法は成功確率を追うシステム解析手法であり、時間経過に伴うシステム信頼度の推移の算定が容易にできるもので、システムを GO-FLOW チャートへモデル化することにより容易に解析できる手法である。各装置の信頼度や故障率をモデリングされたシステムに入力することにより、そのシステムの安全性・信頼性を定量的に求めることができる。

○エレベーターのＦＭＥＡ試行（概要）

１．目的

エレベーターの安全システムの設計・評価を支援する信頼性評価システム開発を目的とし、基本事項・関連事項の調査、とりまとめを行なった。

２．メンテナンス及び利用者の利用方法に依存する事項・内容の明確化

メンテナンス及び利用者の利用方法に依存する事項・内容の明確化を行なう目的で、日本建築設備昇降機センター報告書（エレベーター及び遊戯施設等の安全性能確保のための制御システム等に関する調査検討業務、平成２１年３月）記載の昭和６０年～平成２０年の期間日本において発生した事故不具合の具体的事例について検討した。

対象とした事故不具合は、乗場から昇降路へ転落、かごから転落、かごと乗場の床・天井との挟まれ、戸の開閉による挟まれ、昇降路内機器・昇降路壁等との挟まれ、手足・リード等の挟まれ、閉じ込めである。

信頼性評価の対象事象としては、「戸開走行」、「落下」、「挟まれ」を対象としているため、上記の関連事例を検討し、どの様な部品・機器の不具合が事故に至る可能性があるかを明らかにした。また、使用者の誤操作等に起因する事故も多分にあり得ると想定されるので、事故発生の状況についても、事例の記述をもとに検討を行なった。

検討にあたっては、エレベーターに関する一般の書籍・資料の他に日本建築設備昇降機センター発行の「昇降機検査資格者講習テキスト２００８」及び同センターから入手した資料※）も参考とした。

検討の結果、戸開走行保護装置、特定距離感知装置の安全保護装置の故障･不具合が事故に至る原因となると判断されたので、この構成図の各部品の故障発生時の影響を FMEA（故障モード及び影響評価解析）により検討した。安全保護装置以外の通常運転に関係した機器では、運転制御プログラム、電源、ブレーキ、巻上機、センサーの故障による事例が摘出されたので、これらについても FMEA を実施した。

また、使用者の誤操作等が関与する事例についても FMEA 表に準拠した形式でまとめ、事項･内容の明確化を行なった。

その結果を基に、主として戸開走行、挟まれ、落下事象を対象として集計表を作成した。

※）エレベーターの全体構成図、油付着防止構造図、巻上機構造図、巻上機およびブレーキの構造図、ブレーキ構造図、ブレーキの油汚損防止構造図、位置検出器と遮へい板の関係図、特定距離感知装置の構成図、戸開走行保護装置の全体構成図。