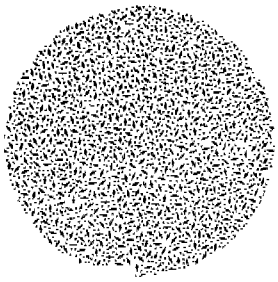
産業災害解析에 있어서 缺陷樹法의 應用

Application of Fault Tree Analysis to Industrial Accidents



李 根 喆

本協會編修委員

1. 序 言

最近 災害가 大形化되고 災害原因이 複雜化 됨에 따라서 各 分野에서 시스템 安全이라는 말을 使用하게 되었다. 시스템安全을 達成하기 위하여는 시스템의 計劃, 設計, 製造 및 運用등의 全段階를 通해서 시스템에 대한 安全管理와 安全工學을 明確히 適用할 必要가 있다.

시스템의 安全管理란 첫째 시스템安全에 必要한 事項의 同定과 安全活動의 計劃, 組織 및 管理 둘째로는 他의 시스템프로그램領域과의 調整 그리고 시스템安全의 目標를 有效하게 適時에 實現하기 위하여 프로그램의 解析, 檢討 및 評價등의 시스템安全業務를 遂行하는데 필요한 프로그램管理의 한 分野이다. 한편 시스템安全工學이란 科學的, 工學的原理를 適用해서 시스템內의 危險性을 適時에 同定하고 이것을 豫防 또는 制御하기 위한 시스템工學의 一分野로서 시스템安全工學은 시스템의 安全性을 明示, 豫測, 評價하기 위하여 工學的 設計와 安全解析의 原理와 手法을 基礎로함과 同時에 數學, 物理學 및 關聯科學分野의 專門的知識과 特殊技術로서 成立되었다고 말할 수 있다.

그런데 시스템安全프로그램에는 시스템의 安全을 實行하기 위한 基本으로서 計劃의 概要와 安全組織 契約條件, 關聯部門과의 調整, 安全基準, 安全解析 및 安全性의 評價등을 包含시킬 필요가 있는데 本稿에서는 FTA의 接近方法과 應用例를 들어서, 簡單히 說明하고자 한다.

2. FTA의 目的과 順序

大規模시스템의 信賴性과 安全性을 解析하기 위한 方法으로서 FTA (Fault Tree Analysis, 缺陷樹法, 缺陷關連樹法 및 故障의 木解析法등으로 飜譯됨)가 있는데 이것은 1961年 Bell 電話研究所의 Watson氏가 미느트멘미사일發射制御시스템에 관한 空軍契約에 關聯하여 最初로 考案한 것으로서 그 後 同 研究所의 Mearns氏를 中心으로한 研究구룹에 의해서 改良되었으며 이것이 미사일의 偶發事故를 豫測하는 問題解決에 크게 貢獻하게된 것을 비롯해서 超音速機 各種交通시스템, 原子力發電플랜트 및 化學프로세스시스템등에의 適用을 위시해서 大規模시스

템의 安全性解析을 行하는 手法으로 確立되어 큰 成果를 올리고 있다.

그런데 FT(Fault Tree)는 AND와 OR의 2種類 論理게이트의 組合에 의해서 對象플랜트設備의 危險性이나 不信賴性의 成立을 表現하는 것으로서 이 表現法은 自体로서 對플랜트設備에 潛在하는 固有의 特徵을 視覺的으로 捕促하는 手段임과 同時에 專門技術分野의 情報를 總網羅하는 柔軟性이 豊富한 시스템的 手法으로서 最大의 特徵은 FT가 對象플랜트의 危險性이나 不信賴性에 관해서 確率論的인 定量性의 議論을 可能케하는 點이라는 것이다.

즉 트리(木)의 基本事象에 대한 發生率이나 Unavailability의 값을 賦與함으로써 트리의 上位에 있는 特定의 中間事象이나 最終 頂上事象의 發生率이 逐次的으로 計算될 수 있는데 이 결과 從來 感覺的 經驗的으로 論議되어온 이런 種類의 問題에 確率論的 定量性을 基礎로한 하나의 길로 接近하게 되었다.

FTA(Fault Tree Analysis)는 一部 對象分野에서 오래전부터 사용되어왔으나 各對象分野에서 導入되기 시작한 것은 最近의 일로서 檢討對象에 따라서 트리의 構成에 理論上 不適合한 問題를 包含하고 있을뿐만 아니라 實用上 약간의 難關에 直面하는 경우가 많아서 適用時 틀리기 쉬운 點이 있다고 한다.

FT에 의한 解析目的은 플랜트나 시스템에 의한 發生事象을 原因側으로 돌리고 多岐에 걸친 因果關係의 連鎖를 統一的 表現으로서 分析評價하는 것이다.

또한 裝置產業으로본 事故災害는 그 發生 要因이 多岐에 걸쳐서 潛在하고 設計나 오퍼레이션의 盲點을 指摘하는 形態로 發生한다. 따라서 事故災害가 發生해서 設計나 오퍼레이션의 不備不適에 알맞게 되는 경우가 많고 이에 대한 對策은 잘못하면 事故의 後追的인 것이 되는데 이러한 事故災害는 여러가지 潛在要因中 어떤 것이 顯在化되므로 其他에도 各種 潛在原因이 存在하게 된다.

한편 裝置設備에는 약간의 特有한 危險性의 形態가 存在하는데 여기에는 裝置의 種類와 形態, 取扱物質, 오퍼레이션 條件, 裝置環境 및 類以裝置의 事故災害事例등으로부터 類推되며 事故災害形態의 種類로는 가스의 火災爆發, 油火災, 裝置 運轉暴走, 有毒가스의 漏出擴散 및 環境汚染物質의 流出 등으로 類形化되고 있다.

그런데 裝置特有의 代表的인 事故災害의 形態가 파악되면 災害想定에 의한 災害規模의 計算과 重要性이 算定되는데 이 中에서 重大한 災害는 그 發生을 未然에 防止하기 위하여 設計上 運轉上의 配慮와 對策이 要求되며 또한 事故災害와는 直接關係가 없으나 裝置의 運轉을 所定期間에 所定의 能力으로 連續維持하는 것이 매우 强하게 要求되는 경우가 있다고 한다.

이를 위하여 裝置의 다운타임을 줄이도록 構成要素의 選定과 시스템 構成에 세심한 배려가 필요한데 FTA에 대해서도 그 適用 範圍와 目的은 各各다르다. 最近 大規模化한 시스템이나 設備에 있어서도 信賴性과 安全性에 대한 要求가 높아지고 있는데 이들 시스템이나 設備는 複雜化, 高性能化 되어가고 있는 反面 여기에서 發生하는 故障은 複雜化되어가고 있다.

FTA는 시스템이나 設備의 信賴性解析과 安全性解析에 使用되고 있으며 信賴性과 安全性은 密接한 關係에 있으나 반드시 一致하지 않고 있다. 信賴性은 하드웨어, 소프트웨어 및 人間要素를 包含해서 對象이 되는 시스템이나 設備가 본래의 機能을 健全하게 發揮하도록 하고 있으며 한편으로 安全性은 시스템이나 設備의 事故가 結果로서 人命의 喪失이나 傷害의 發生으로 進展하는 事態를 未然에 防止하는 것을 말한다.

그런데 生產라인의 本來機能은 所定의 生產을 維持하는데 있으나 이 稼動性과 安全性은 반드시 一致하는 것이 아니며 한편 安全性을 確保하는 目的으로 設置된 防災設備는 信賴性의 向上과 安全性의 向上에 連結되고 있다. 安全性解析에서는 安全性에 關與하는 部分機器나 오퍼레이터의 信賴性解析이 包含되어 있으나 플랜트의 正常運轉을 위한 維持解析과 檢討해야할 範圍는 最終目的과는 다르다. 또한 安全解析을 目的으로 하여도 基本的인 考察方法과 檢討順序는 거의 同一하며 FT에 의한 解析은 對象시스템의 性質이나 解析의 目的 및 等級에 의해서 多少 差異가 있으나 標準的인 面에서 다음과 같다고 말할 수 있다.

Step. 1. 頂上事象의 設定

플랜트로서 豫想되는 重大事故나 危險狀態가 FT

의 頂上事象으로서 設定된다. 이 設定을 위해서는 플랜트에 事故가 發生하는 경우에 대해서 災害想定을 行하고 重要하다고 生覺되는 事象을 選定한다.

특히 安全性解析의 경우에는 事故災害의 類形化를 充分히 吟味하고 事故의 發展 過程을 圖表化 해서 整理하는 것이 解析에 便利하다.

Step 2. 對象플랜트의 特性把握

시스템의 內容이나 特徵을 裝置의 設計面이나 運轉面에서 充分히 이해한다. 이때문에 裝置의 設計資料와 運轉메뉴얼을 檢討吟味하고 특히 安全上 配慮되고 있는 要點을 整理해서 충분히 파악한 다음 頂上事象을 발생시키는 原因側의 中間事象을 널리 分析하고 그 결과를 정리한다. 이것을 다시 原因側의 事象으로 展開하는데 특히 異常發生과 檢知, 對處의 關聯을 識別整理해서 부분적인 因果關係를 部分的인 FT로 다시 쓰는 것이다.

Step3. FT의 作成

一般的으로 FT는 각종 事象과 이것을 連結하는 게이트에 의해서 構成되는데 먼저 解析해 야할 災害(Top event 頂上事象 또는 目標事象)을 쓰고 그 下段에 災害의 直接原因이 되는 機械와 設備의 不良狀態나 作業者의 에러등(Fault event, 缺陷事象) 을 並記하고 頂上事象間을 게이트로 連結한다.

다음에 여러 가지 缺陷事象의 直接原因이 되는 缺陷事象을 3번째에 쓰고 2번째사이를 게이트로 연결한다.

Step4. FT의 構造分析

FT의 圖的構造는 自体로서 많은 重要한 情報를 包含하고 있으며 트리의 全体와 部分의 關係를 吟味함으로써 圖的構造로부터 重要한 中間事象을 抽出할 수 있다. 그런데 共通의 原因事象이 트리로 複數個所에 나타날 경우 그 原因事象을 共通모우드라고 부르며 解析上 注意를 要한다. 이와같은 경우에는 Boole變換이라고하는 明確한 論理原則을 사용해서 여러 가지 等價인 트리를 作成할 수 있다.

Step5. FT의 定量化

트리末端의 原因事象에 대한 發生頻度나 Unavailability를 주기 위하여 類似한 機器의 故障率 데이타나 오퍼레이터의 에러데이터를 適當한 값으로 設定하고 트리의 上位事象에 대하여 順次的으로 定量化計算을 推進한다. 그런데 트리全体의 定量化가 終了할 경우에는 中間事象의 確率값을 상호 비교함으로써 絶對値에 부당한 大小가 있는가를 체크한다.

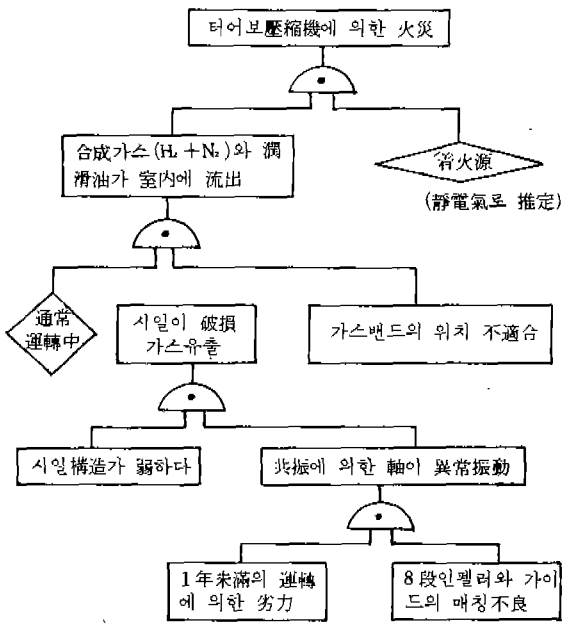
Step 6. FT의 解析結果評價

算出되는 頂上事象의 發生頻度는 事象의 重大性으로보아 許容될 수 있는가를 評價한다. 한편 許容될 수 없거나 發生頻度를 減少시킬 수 없을 경우에는 어떤 部分의 改良이 효과적인가를 檢討한다. 檢討時에는 FT의 구조를 조사하고 中間事象의 값을 比較分析하는 것이 有効하다.

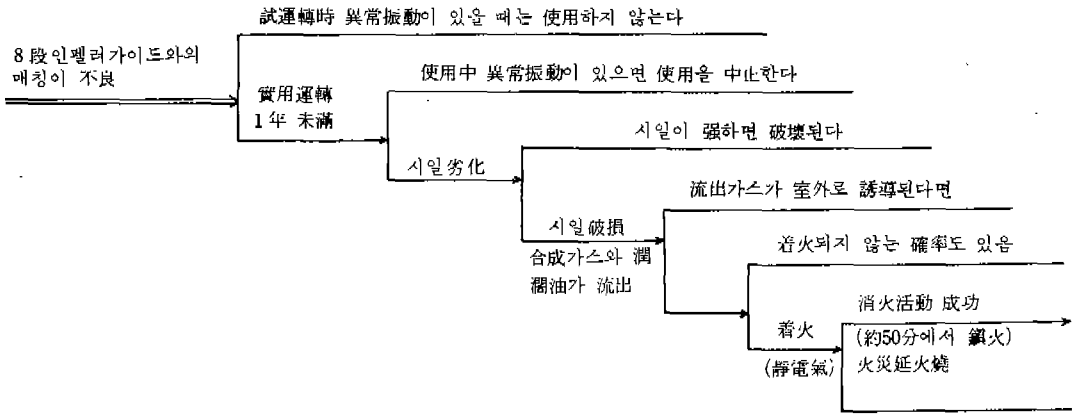
이 때문에 頂上事象에 대한 各種 原因事象의 寄與度를 조사하고 이들 頂上事象의 感度解析을 實行한다. 이것으로부터 改良의 효과를 평가하나 一部 트리의 轉換이 필요하게 된다. 그러나 對策 選定에는 經濟性, 保全性, 操作性을 勘案한 케이스스터디가 된다.

3. 高速回轉機械에 의한 災害事故

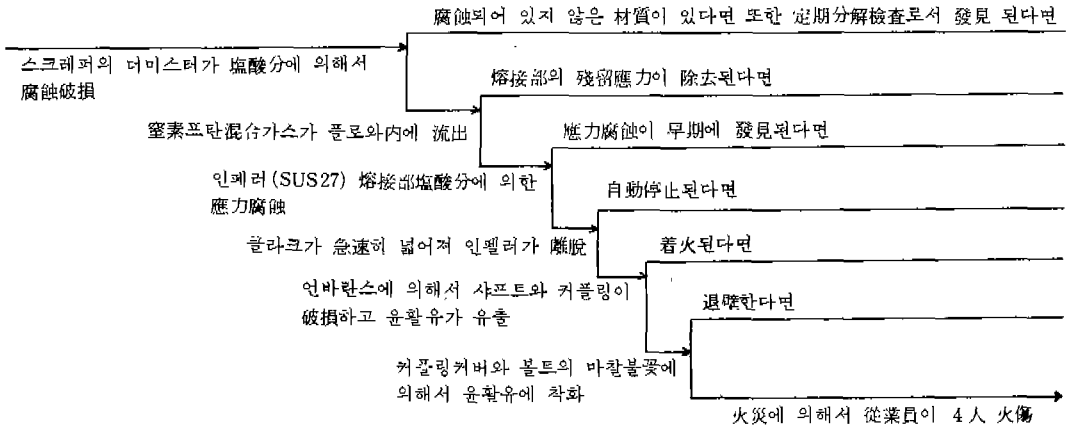
그림 1은 8段터어보壓縮機에 의한 火災事故를 F



〈그림－1〉 8段터어보壓縮機에 의한 火災事故의 FTA



〈그림－2〉 8段터어보壓縮機에 의한 火災事故의 ETA



〈그림－3〉 폴리프로필렌플랜트에 있어서 窒素循環送風機에 의한 火災事故

TA에 의해 나타낸 것이고 **그림2**는 同一한 災害事故를 ETA(Event Tree Analysis)로 表現한 것으로서 FTA에 의한 災害事故의 原因을 다음과 같이 分析할 수 있다. 첫째는 8段인펠러와 가이드의 매칭이 不良이고 둘째로는 시일의 構造가 弱하고 세번째로는 가스밴드의 位置가 不適合하다는 것이다. 따라서 그림2의 ETA에 의하면 8段인펠러와가이드의 매칭을 알 수 없어도 試運轉과 實用運轉段階에서 振動의 異常診斷技術이 있다면 火災事故를 豫防할 수 있다고 한다.

또한 **그림3**은 폴리프로필렌플랜트의 窒素循環送風機에 의한 火災事故를 ET로 分析한 것으로서 이 事件은 最惡條件의 連續的 累積에 의해서 發生한 災害事故의 典形的인 事例이다.

以外에 各種 災害事故例 즉 石油탱크, 配管, 化學工場의 爆發, 粉塵爆發, 自動運送機, 切削加工中의 重傷 및 死亡事故 및 프레스에 의한 死亡事故를 FTA로 나타낸 例는 紙面關係上 省略하기로 한다.

*