天文観測システムの開発プロジェクトにおける安全プログラムの概要

太田政彦（国立天文台 安全衛生推進室）

概要

観測装置のシステムが複雑化するに従って潜んでいるハザードを見出すのが困難になることから、開発・設計段階でハザード解析などを実施して、その結果を設計審査/安全審査にて組織的に評価し、安全性を高める手法が広く浸透してきている。国立天文台ではＡＬＭＡ或いはＴＭＴプロジェクトにてこの安全プログラムを導入しリスクの低減に活用しているので、その概要を紹介する。

1. 開発プロジェクトの安全プログラム

国立天文台のミッションの一つに「知の地平線を拡げるため、大型研究施設を開発・建設し、共同利用に供する」が挙げられている。従ってかつてより大型研究装置を含めた各種のプロジェクトが数多く立ち上がっている。それらの装置は危険要素を孕んでいるものが多く、大型装置の望遠鏡を例にとると回転作動、重量物、高所作業等々があり、高地低酸素環境に設置されるものは作業者の思考能力、身体能力が減退させる危険性があるので、高い安全管理レベルが要求される。このプログラムは、それらの装置の全体システム、サブシステム、コンポーネントなど広い範囲で活用できるものである。

2. 審査要求/安全要求の文書体制

ALMA プロジェクトを例に取ると、安全プログラムの推進のために以下の様な文書体制を敷いて解析、審査の実施と安全の要求を明確にしている。

(1) 安全を含む設計審査の実施と安全評価報告書等の安全関連文書を要求する文書
(2) ハザード解析などの解析実施を要求する文書
(3) 電気、機械、制御、防護、表示などの一般的な安全設計要求の文書
(4) 具体的な安全設計要求が示されている装置仕様書
(5) ジョブハザード解析を実施し、サイトの建設や運用における作業の安全を要求する文書
(6) その他

3.安全プログラムのイメージ

安全プログラムをイメージするために、図１にフローチャートにて視覚的に表した。

システム仕様設定時には安全と装置の機能・性能の基本要求仕様を明確にし、装置設計段階でそれらを図面化するが、設計時には安全解析、信頼性解析等々を行いながら設計内容を基本要

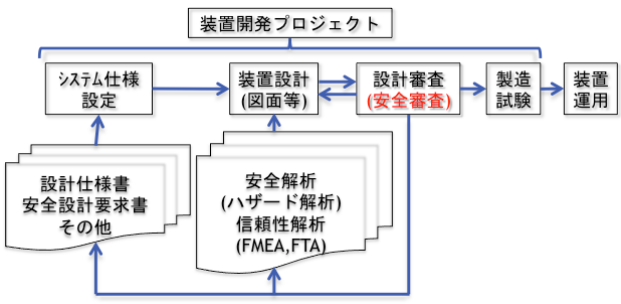

図１安全プログラム

求仕様に合わせていく。その後、設計審査会/安全審査会にて安全と要求仕様が正しく装置設計に反映されていることを審査、評価する。開発・設計内容が審査者に承認されると次フェーズの製造へ移行することが出来る。設計審査/安全審査はその上流部分をきめ細かく見張っていることになる。この様にして安全の設計品質を高めていくのが開発プロジェクトの安全プログラムと考えている。

4.安全設計・解析と審査の過程

設計の過程は表１に示すように、初期の基本設計段階と設計内容を確定する後期の詳細設計段階とで構成する。前者は基本設計審査(PDR)、後者は詳細設計審査(CDR)を安全審査を含めて開催し、安全解析と信頼性解析などの結果を審査する。安全審査は独立して開催しても構わない。安全解析と信頼性解析の結果と安全評価報告書は、基本設計段階から詳細設計段階に移行するときには見直して最新化する。

表１設計と審査の過程

	基本設計	詳細設計	製造～出荷
安全審査	ﾌｪｰｽﾞ1 SR	ﾌｪｰｽﾞ2 SR	
安全解析	ハザード解析 ①ハザード及び原因の確認 ②ハザードの制御方法の確認 ③ハザード検証方法の確認	ハザード解析の更新 ①ハザードの制御方法が設計上実現されていることの確認 ②ハザードの検証方法の詳細が設定されていることの確認	①検証結果の追跡 ②発覚した不安全はハザード解析に反映
報告書作成	安全評価報告書(9項参照)	同左(更新)	
設計審査	基本設計審査 PDR	詳細設計審査 CDR	
信頼性解析	FMEA, FTA他	同左(更新)	
製造以降			MRR, PSR

5.安全審査実施体制･実施方法

安全審査は審査側と受審側に分かれて、前者は議長、審査者（場合によっては外部審査者を含める)、後者は発表者、設計者、安全管理者、その他の関係者が参加し実施する。審査文書としてハザード解析結果、FMEA 結果、FTA 結果などの安全関連資料を準備し、審査者は事前配布された資料を審査する。審査者は指摘を設計者に送付し、設計者等はその指摘に対する対応策を安全審査時に説明して了承を求める。審査者が全部の回答を承認すると次フェーズへの移行が認められる。

6.ハザード解析の概要

この解析の結果は安全審査の審査対象として最も重要な資料である。そこにはハザード（事故をもたらす要因が顕在又は潜在する状態）が現実化した場合のリスクのレベルと、その安全対策、その検証方法が論理的に述べられている。即ち簡単に述べると「潜在的なハザードが現実化したらどの程度のリスクとなるかを見極めて、それ相応の対策を事前に講ずる。」ものである。

6.1 装置に潜在するハザードの識別方法

潜在するハザードを掘り起こして事故の未然防止をいかに確実なものにするか、大変重要なステップであるので、熟考して推測すると同時に、次の３種の方法を活用する。

(1) ハザードチェックリストの活用。

(2) FMEA（機能）の不安全モードを取り上げる。

(3) FTA のハザード事象を取り上げる。

6.2 リスクの許容の判定

前項で識別したハザードに対して表２リスク許容判定基準を活用して、リスクレベルを判定する。「許容出来ない」、「許容可否判断要」を識別されたものは十分な安全対策を検討する。太枠内のリスクに該当するものはハザード解析フォームで解析を実施する。

表２リスク許容判定基準

発生の可能性【Probability】	被害の度合い【Severity】 1.破局（Catastrophic）	2.重大（Critical）	3.限界・局所的（Marginal）	4.無視可能（Negligible）	備考
A.しばしば発生する（Frequent）	1A	2A	3A	4A	
B.たまに発生する（Probable）	1B	2B	3B	4B	
C.まれに発生する（Occasional）	1C	2C	3C	4C	
D.殆ど発生しない（Remote）	1D	2D	3D	4D	
E.殆ど全く発生しない（Improbable）	1E	2E	3E	4E	

凡例 ：許容出来ない ：許容可否判断要 ：許容範囲
：HR 作成の範囲（HR：Hazard Report）

6.3 ハザード解析フォーム

ハザード解析を実施するには図２のフォーマットを用いる。ここに記載された項目通りに記載していけば良いのであるが、⑩～⑭を簡単に説明する。

⑩ハザードが現実化したときの現象
⑪上記⑩の現象の原因
⑫その原因によって生じるハザードに対する、除去、軽減し安全化する制御方法
⑬制御方法が適切に実施されていることの検証方法
⑭検証の完了状況

Hazard Report		①No.	
②Product		③Phase	④Date (Y.M.D)
⑤Subsystem	⑥Hazard Group		
⑦Hazard Title			
⑧Applicable Safety Requirements		⑨Hazard Category	
		Severity	Probability
⑩Description of Hazard：			
⑪Hazard Causes：			
⑫Hazard Control：			
⑬Safety Verification Methods：			
⑭Status of Verification：			

図２ハザード解析フォーム

6.4 安全設計対策の要点

ハザードが現実化したときの被害の度合が「破局」、「重大」に該当するものは、安全設計対策（制御方法）の数を前者は３段階以上、後者は２段階以上を設計に組み込む故障許容設計を適用する。前者を二重故障許容設計(2FT)、後者は単一故障許容設計(1FT)と呼ぶ。それ以外はフェールセーフ設計(0FT)を行う。安全審査時にはこれを満足する設計となっているかを、審査者は審査しなければならない。

故障許容設計には冗長設計とインヒビット設計があり、前者は「機能が常時作動していなければならない場合」、後者は「機能が定まったとき以外に作動してはならない場合」に用いる。

7. 安全評価報告書の作成

プロジェクトの安全審査後には全体を纏めた報告書を作成する。安全設計内容と評価結果の概要を記載し、特に識別されたハザードが安全上適切に対処され確認されたことを、補足資料を使って説明する。安全審査のフェーズが進んだときには、これを更新する。

8. ジョブハザード解析の概要

前項までは開発･設計段階の安全プログラムについて説明したが、この項は実験、製造、組み立て、検査、運用･保守などに含まれる危険作業に関する解析手法を示す。これはヒヤリハットが後追い対策であるのに対し、事前対策が特長である。ハザード解析同様、チェックリストを用いてハザードを識別し、「被害の度合」をランク付けし、表３の解析フォーマットを活用して制御･対策の方法を検討する。その対策を行った上で作業を開始することを、責任者に申請書を用いて許可を依頼し、承認された後に作業を開始するものである。

表３解析フォーマット

No	ハザード タイトル	潜在 ハザード	被害の 度合	ハザードの 原因	ハザードの制御・対策
1					
2					
3					

9. 不具合・事故発生時の対応

不具合･事故が発生した場合には、課題報告書（又は不具合報告書、NCR）を用いて、その場の対策と再発させないための今後の対策を検討して報告書に纏める。この報告書には次のアイテムを記述する。

(1)不具合内容　　不具合･事故の経緯と事象

(2)不具合原因　　根本原因・発生メカニズム

(3)処置内容　　対策処置内容

(4)再発防止処置　　恒久的な再発防止対策

なお、根本原因を分析する場合は FTA を活用するとよい。開発･製造委託業者が不具合、事故を起こした場合にも、この報告書と FTA の提出を求めて精査するとより正しく原因が把握でき、確実な対策を講ずることが出来る。

10. おわりに

この安全プログラムを系統立てて説明したことは無かったので、技術シンポジウム開催の機会を捉えて紹介出来たことは幸いであった。これは技術者の方達が主体となって推進して頂かねばならない内容であるので、今後のプロジェクトの立ち上がり時、或いは平素の業務における装置の開発時に是非応用して頂きたい。そしてこのプログラムが天文台内に定着し、事故の未然防止に役立つことを期待している。

以　上