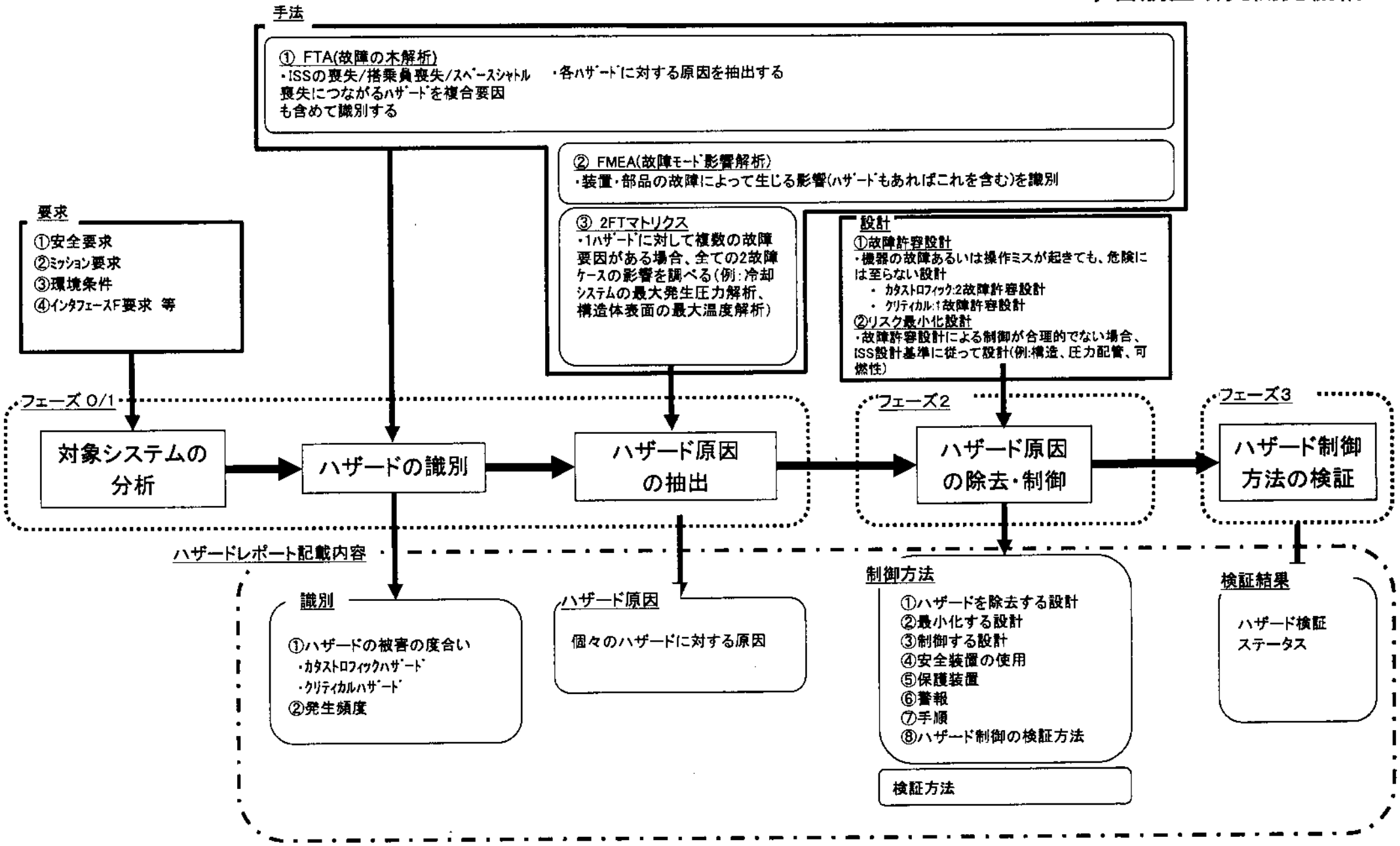
安全設計の流れ


手法
① FTA(故障の木解析)
・ISSの喪失/搭乗員喪失/スペースシャトル喪失につながるハザードを複合要因も含めて識別する
・各ハザードに対する原因を抽出する
② FMEA(故障モード影響解析)
・装置・部品の故障によって生じる影響(ハザードもあればこれを含む)を識別
③ 2FTマトリクス
・1ハザードに対して複数の故障要因がある場合、全ての2故障ケースの影響を調べる(例:冷却システムの最大発生圧力解析、構造体表面の最大温度解析)
設計
①故障許容設計
・機器の故障あるいは操作ミスが起きても、危険には至らない設計
・ カタストロフィック:2故障許容設計
・ クリティカル:1故障許容設計
②リスク最小化設計
・故障許容設計による制御が合理的でない場合、ISS設計基準に従って設計(例:構造、圧力配管、可燃性)
要求
①安全要求
②ミッション要求
③環境条件
④インタフェースF要求 等
フェーズ 0/1
対象システムの分析
ハザードの識別
ハザード原因の抽出
フェーズ2
ハザード原因の除去・制御
フェーズ3
ハザード制御方法の検証
ハザードレポート記載内容
識別
①ハザードの被害の度合い
・カタストロフィックハザード
・クリティカルハザード
②発生頻度
ハザード原因
個々のハザードに対する原因
制御方法
①ハザードを除去する設計
②最小化する設計
③制御する設計
④安全装置の使用
⑤保護装置
⑥警報
⑦手順
⑧ハザード制御の検証方法
検証方法
検証結果
ハザード検証ステータス