様式Form

論　文　内　容　の　要　旨
Abstract of Dissertation

氏　名Name　柴垣　光男

本論文は，あるシステム（系）のハザード（Hazard）を体系的・系統的に洗い出し，その結果から合理的かつ系統的に抑制策を導出し，さらに抑制策の適用に関して相反ハザードの有無を識別する方法を議論している。

本論文では，相反事象及び相反事象で構成される相反ハザードに着目する。1 つの事象があるハザードに対して危険側であり，他方のハザードに対して安全側である場合，これらのハザードを当該事象に関して相反ハザードという。例えば，自動車の走行では追突するハザードと追突されるハザードがある。プリクラッシュシステムの故障による誤停止は追突するハザードに対して安全側であるが,追突されるハザードに対しては危険側である。これらのハザードは，誤停止に関して相反ハザードである。また，その危険側事象は，故障, エラー, 失敗等の無秩序状態作用だけでなく, システム要素の正常な要求機能の履行，修復，回復等による秩序状態作用によって行われる可能性が存在する。

相反ハザードの生成は事象の生起順序と強い相関があり，相反ハザードの同定及び分析にあたっては，ハザード生成過程の動的検討，すなわち危害発現プロセスを次々と変化する状態及び事象の連鎖として把握することが必要である。ハザードを同定・分析するための従来技法，例えば，HAZOP（Hazard and Operability）スタディーズ，FTA（Fault Tree Analysis）, ETA（Event Tree Analysis）, FMEA（Failure Modes and Effects Analysis）等が，自動車，ロボット，産業機械等の分野で幅広く適用されてきた。しかしながら，これら従来技法は，危害に至る危害発現プロセスにおける状態と事象との関係及びその生起順序を系統的に同定して図式化する手段を持たず，相反ハザードの分析には不十分な側面をもつ（**第 1 章，第 2 章**）。

この課題に対して本論文は，まず**第 3 章**において，状態と作用の生起順序に着目したハザードの図式表現による S-A プロセスチャート（State-Action Process Chart）手法を提案すし，ハザードを図式表現するための S-A プロセスチャートの理論的枠組みと構築方法について論じている。さらに次章以降でその有効性を論じている。

第 4 章では，　環境試験槽の停止及びリチウムイオン 2 次電池の熱暴走に起因するハザードの同定とその抑制策の導出に S-A プロセスチャートを適用している。その結果，(a) システムのそれぞれの状態にシステム要素の故障（無秩序状態作用）だけでなく，正常機能の履行（秩序状態作用）によって起こる遷移作用を順次作用させることによって，危害に至る状態遷移プロセスを系統的に追跡し，ハザードの網羅的同定が可能であること，(b) 図式化されたハザードの状態と遷移作用の配列構造からハザードの抑制策を合理的かつ系統的に導出することが可能であることを検証している。

第 5 章では，事例としてガス爆発及び自動車の追突に関して，すでに特定された危害と初期状態とを結ぶ状態遷移経路の分析に S-A プロセスチャートを適用している。まずシス

テムの状態をシステム要素が持つ状態の組合せによって定義し，各システム状態の遷移可能な経路と遷移作用が，状態遷移経路図で表現されることを示している。次に，この状態遷移経路図上で初期状態と危害とを結ぶ経路をたどることによって，状態遷移経路が異なるハザードが網羅的・系統的に洗い出される。その結果，ある状態では抑制作用（安全側事象）となり，別の状態では危害を発現させる作用として働く事象（危険側事象）を S-A プロセスチャート上で識別し，相反ハザード等の分析に対する S-A プロセスチャートの有効性が検証されている。

第 6 章では，まず S-A プロセスチャートから得られたハザードを，優先 AND 構造を持つ FT（S-A-FT）で展開する手法を提案している。次に，2 冗長電源システムの故障に至るプロセスの分析に本技法を適用し，S-A-FT では S-A プロセスチャートと FTA とが互いに補完的役割を担うことによって，システム要素レベルまでのハザードのより合理的な分析が可能となることを示している。

第 7 章では，本研究を総括し，本研究で明らかにした（a）~（d）を結論として示している。

(a) システム状態が状態を変化させる作用を伴う事象によって次々と遷移し到達し得る危害の同定，すなわちハザードの網羅的同定が可能である。

(b) 網羅的に同定したハザード群の中から相反ハザードの識別が可能である。

(c) 相反ハザードの抑制策の合理的かつ系統的な導出が可能である。

(d) S-A プロセスチャートを S-A-FT で展開し，より合理的なハザード/リスク分析が可能である。

以上，要するに本研究による S-A プロセスチャートは，有用でありその適用範囲は広い。