参考資料5　欧州安全規格に定められたカテゴリ方式による故障対策

欧州安全規格では，システムの故障解析を実施するにあたり，ＥＮ１０５０に基づいてリスク・アセスメントを行い，この結果を基に故障対策のカテゴリを与えている。このような評価方式をとるために，欧州安全規格の下では，一般に機械の危険性が高くなるに従い，より高い水準（カテゴリ）の故障対策を選択することになる。

表１は，欧州安全規格ｐｒＥＮ９５４－１[1)]で定められている制御システムのカテゴリである。

表１　欧州安全規格におけるカテゴリ

カテゴリ	必　要　条　件	システムの挙動
B	・使用条件や予測される作用（たとえば，原料の影響，振動，電源中断）に耐える設計	・故障で安全機能を失う ・検出できない故障が残る
1	・カテゴリＢの条件が適用される ・従来から多く使用（テスト）されてきたか，十分吟味した安全原則（たとえば，特定故障の回避，故障の影響の限定，早期故障検出，ディレーティング等）を使う	・Ｂと同様であるが，信頼性は高い
2	・カテゴリ１の条件が適用される ・適切な間隔で（最低限始動時に）安全機能が検査される ・始動時検査は，システムにより自動的に実行されるか，または人が行う ・検査出力は，故障のないとき運転を許可するか，または故障時安全側となる ・検査装置には，カテゴリＢ以上の要件が適用される	・故障は検査により検出される ・故障発生後，次の検査までの間は安全機能が失われることがある
3	・カテゴリ１の条件が適用される ・単一故障により，安全機能は失われない ・技術的に可能ならば，単一故障は検出される	・単一故障の発生時には，安全機能が常に実行される ・（全てではないが）故障は自動的に検出される ・検出されない故障の蓄積により，安全機能を損なうことがある
4	・カテゴリ１の条件が適用される ・単一故障により，安全機能は失われない ・単一故障は，技術的に可能ならば検出されるか，次に安全機能が必要となる前には検出される ・故障検出が不可能な場合でも，故障の蓄積による安全機能の消失はない	単一故障発生時には，安全機能が常に実行される ・安全機能が損なわれる前に故障は適時自動的に検出される

文献１）欧州安全規格　ｐｒＥＮ９５４－１（1993）