付表： 安全カテゴリ

■安全カテゴリとは

国際安全規格では、安全に関わる制御システムの不具合（障害）発生時における安全機能維持の耐性を確保するため、一般に考えられる「品質を上げて故障しないようにする」だけではなく、「定期的に故障の有無をチェックする」、「故障しても安全機能を維持させる」、「故障を検出したら運転させない」というように、はじめから故障することを認めて安全を確保する考え方が盛り込まれています。

リスクの評価に基づき、安全を確保するための機能（安全機能）を決定する上での指標として、制御システムの安全関連部を規定するＩＳＯ１３８４９－１では、安全に関わる制御システムが故障した場合の安全機能の維持能力を分類しています。
これを安全カテゴリと呼んでいます。

■安全カテゴリ分類と必要要件　－ＩＳＯ１３８４９－１に基づく－

分類（カテゴリ）	要件の要約	安全機能の維持能力（抵抗性）	安全性を達成するための原則
B	●機械制御システム安全関連部の目的機能を実現すること （目的機能で考慮すべき使用状況下のストレスの例） ・遮断容量および遮断頻度に関する信頼性 ・洗浄機の洗浄剤のような処理材料の影響 ・機械振動、外部磁界、動力源の中断または妨害のようなその他の関連した外部の影響 注）カテゴリBに適合する部分には特別な安全方策は、適用しない	故障発生時安全機能を損なう場合が十分起こりえる	主に構成部品の選択による
1	●カテゴリBの要件を満たすこと ●十分吟味された高信頼性のコンポーネントを使用し、安全の確保は安全原則に従うこと （十分吟味された高信頼性のコンポーネントとは？） ・従来、同じ適用において安全上で良好な結果であると共に、広く用いられてきたもの ・安全関連の適用に対するその適切さおよび信頼性を示す原則を用いて製作され、検証されてきたもの （安全原則の例） ・分離による短絡回路の回避のような必然的な故障の回避をする。 ・構成部品の大型化または定格以下での使用のような故障可能性の低減をする ・故障モードの方向付け、たとえば、故障時に電源遮断を必須とする場合、確実に断路する ・故障発見 ・故障の影響の大きさの制御たとえば、設備の接地	カテゴリBと同様であるが、安全関連部の安全確保機能の信頼性は高い	

分類（カテゴリ）	要件の要約	安全機能の維持能力（抵抗性）	安全性を達成するための原則
2	●カテゴリBの要件を満たすこと ●安全の確保は安全原則に従うこと ●安全機能が適当な間隔でチェックされること （安全機能のチェック） ・機械の起動時および全ての危険状態が始まる前に行う ・リスクアセスメントと操作の種類が定期点検の必要性を示している場合、操作中に定期的に行う （安全機能のチェックは自動でも手動でもよいが、チェック項目は以下のいずれか） ・故障が発見されなければ操作が可能である ・故障が発見されれば、適切な制御作用の開始出力を発生する、可能な場合はいつでも、この出力は安全状態をつくりだす ・安全状態を発生することが不可能な場合（たとえば、最終のスイッチ装置における接点の溶着）、出力は危険警告を出力しなければならない ・故障の発見後、安全状態を故障が解消するまで維持しなければならない ●チェック自体で危険状態に至ってはならない、チェック用装置は安全関連部品に組み込むかまたは分離していてもよい ●安全機能のチェックは、圧力スイッチ、温度センサのようにすべての構成部品に適用できないので、カテゴリ2はシステムによっては適用できない ●一般にカテゴリ2は、保護装置および特殊な制御システムにおけるような電子技術で実現可能である	安全機能の消失はチェックによって検出されるが、チェックとチェックの間では安全機能を損なう場合がある	主に構成による
3	●カテゴリBの要件を満たすこと ●安全の確保は安全原則に従うこと ●設計要件：単一故障で安全機能を損なわないこと 単一故障はできる限り検出されること	●単一故障で安全機能は損なわれない ●すべてではないが、故障の検出ができる未検出故障の蓄積によって安全機能を損なう場合がある	
4	●カテゴリBの要件を満たすこと ●安全の確保は安全原則に従うこと ●設計要件：単一故障は安全機能実行時、もしくはその前に検出されること これが実施できないときは、故障の蓄積で安全機能を損なわないこと	●故障が生じた場合、常に安全機能は損なわれない ●故障は安全機能実施の前の段階で安全機能実施が必ず間に合うように、予防設置として検出される	

本事例の企業発行：「安全コンセプトブック」より抜粋