

安全工学における「3重化(トリプルリダンダンシー)」の考え方

安全の予備 2台法則 2台機械やコンピュータ同時に偶然壊れることはある 3台機械やコンピュータ同時に壊れることはない 3台機械やコンピュータ同時に壊れる時は、欠陥がある スペースシャトルは3台同じ者をツンデいる聞いたことがある本当か

ChatGPT:

おっしゃっている「安全のための予備 2台法則(冗長性の原則)」や、「3台同時に壊れるときは設計や運用に欠陥がある」という考え方とは、航空宇宙、原子力、軍事など高信頼性が要求される分野で広く知られている非常に重要な安全工学の原則です。

安全工学における「3重化(トリプルリダンダンシー)」の考え方:

■ 基本原則:

- 1台:壊れたらおしまい(シングルポイント故障)
- 2台:偶然2台が同時に壊れることは非常に稀 → 安全
- 3台:同時に壊れたら、それは偶然ではなく設計や運用の欠陥があるとみなすべき

このように、「同時に3台壊れることは偶然ではない」という考えは、たとえば航空機や原子炉制御などでも使われており、フォールトトレランス設計(故障に強い設計)においての原則となっています。

スペースシャトルのコンピュータ構成について(事実):

NASAのスペースシャトルには、次のような高度な冗長性を持ったコンピュータシステムが搭載されていました。

■ 主コンピュータ: GPC(General Purpose Computer)

- シャトルには**合計5台のGPC(IBM AP-101S)**が搭載されていました。
- そのうち4台は完全に同一のソフトウェアを実行。
- 残り1台(バックアップシステム)は、別の独立チームが開発したソフトウェア(独立冗長)を実行。

■ なぜ5台?

- 4台中3台の多数決で正誤を判定(フェイルセーフ構成)
- 残り1台(5台目)は異常時のバックアップ用で、異なるコードで動作

この構成は「冗長性 (redundancy) と分離設計 (独立性) を両立」しており、1台や2台が誤動作しても、全体の安全性は確保されるように設計されていました。

✓ まとめ：

- あなたが述べた「3台同時に壊れたら欠陥がある」は、安全設計の基本的な考え方として正しいです。
- スペースシャトルはその原則を採用しており、実際には4台で投票、5台目は独立系のバックアップという構成でした。
- この方式は「トリプル・モジュラ・リダンダンシー (TMR) + 異種冗長」の一例です。