再発見！新発見！

# 計装豆知識

役立つ知識が粒揃い!!

## 機能安全とIEC規格61508について(3)

先月に引き続き、機能安全を規定しているIEC規格61508について説明します。

先月、フェーズ5で各安全機能に対して安全度水準(SIL＝Safety Integrity Level) を割り当てる話が出てきましたが、ここで安全度水準(SIL)について説明しておきます。SILとは、IEC 61508においてシステムの安全性能を表す尺度で、SIL1からSIL4まで4段階定められ、SIL4が最高の水準です。また、**表1**および**表2**に示すように、低頻度作動要求モードと高頻度作動要求モード(または連続モード)の2種類の運転モードにおける、各SILに対応した目標機能失敗尺度が規定されています。

自動車の安全システムを例にすると、低頻度作動要求モードはエアバッグに相当し、安全システムへの動作要求は年に1回あるかないかというものです。高頻度作動要求モードはブレーキに相当し、安全システムへの動作要求は時間当たりや一日当たりに何回というものです。通常、我々のプロセス産業分野では、低頻度作動要求モードが使用されます。低頻度作動要求モードで、作動要求当たりの設計上の機能失敗平均確率とあるのは、エアバッグへの動作要求があった際にエアバッグが動作しない確率の平均という意味です。動作しない確率ですから、最高水準のSIL4では$10^{-5}$以上$10^{-4}$未満という小さな確率の範囲であることが必要とされます。

**表1**の機能失敗平均確率は、PFD (Probability of Failure on Demand) の平均値でPFD$_{AVG}$とも表されます。PFD$_{AVG}$の計算式として最も簡単なシステム、すなわちセンサなどの入力が1つ、アクチュエータなどの出力が1つで、非冗長化構成[注)]の場合の式は下記のとおりです。

$$PFD_{AVG} = (\lambda_{DU} + \lambda_{DD})\, t_{DE}$$

$$\text{平均故障時間：} t_{DE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$$

以下、式に使われているパラメータについて説明します。

**●プルーフテスト間隔(Proof test period)**：$T_1$ (hour)

安全システムの機能が正しく動作しているかどうかを確認するために行う機能確認試験をプルーフテストといいます。プルーフテスト間隔とは、この機能確認試験を実施する時間の間隔のことです。

**●平均修理時間 (Mean time to restoration)**：MTTR (hour)

一般的な信頼性用語の定義と同じで、システムが故障したときに必要になる復旧までの平均時間のことです。

**●故障率 (Random hardware failure rate)**：$\lambda$ ($\lambda_S$、$\lambda_D$、$\lambda_{DD}$、$\lambda_{DU}$、$\lambda_{SD}$、$\lambda_{SU}$)

一般的な信頼性用語の定義と同じですが、PFDを求める必要から次のように分類しています。

**安全側故障率**：$\lambda_S$　　**危険側故障率**：$\lambda_D$

**検出可能な安全側故障率**：$\lambda_{SD}$

**検出不可能な安全側故障率**：$\lambda_{SU}$

**検出可能な危険側故障率**：$\lambda_{DD}$

**検出不可能な危険側故障率**：$\lambda_{DU}$

なお、今回例示した式には使われていませんが、機能安全の理解に必要なパラメータとして、自己診断率があります。

**●自己診断率(Diagnostic coverage)**：DC (%)

危険側ハードウェア故障に対して自己診断テストがカバーする割合のこと。検出可能な危険側の故障率を$\lambda_{DD}$、検出できない危険側の故障率を$\lambda_{DU}$とすると自己診断率DCは次式で表すことができます。

$$DC = \lambda_{DD} / (\lambda_{DD} + \lambda_{DU})$$

機能安全では、危険側故障が少ないほど、また危険側故障が潜在していても自己診断で検出できれば、安全度が高いと評価されます。 ■

表1　安全度水準：低頻度作動要求モードで運用するE/E/PE安全関連系に割り当てられる安全機能に対する目標機能失敗尺度

| 安全度水準(SIL) | 低頻度作動要求モード運用(作動要求当たりの設計上の機能失敗平均確率) |
|---|---|
| 4 | $10^{-5}$以上 $10^{-4}$未満 |
| 3 | $10^{-4}$以上 $10^{-3}$未満 |
| 2 | $10^{-3}$以上 $10^{-2}$未満 |
| 1 | $10^{-2}$以上 $10^{-1}$未満 |

表2　安全度水準：高頻度作動要求又は連続モードで運用するE/E/PE安全関連系に割り当てられる安全機能に対する目標機能失敗尺度

| 安全度水準(SIL) | 高頻度作動要求又は連続モード運用(単位時間当たりの危険側故障確率 [1/時間]) |
|---|---|
| 4 | $10^{-9}$以上 $10^{-8}$未満 |
| 3 | $10^{-8}$以上 $10^{-7}$未満 |
| 2 | $10^{-7}$以上 $10^{-6}$未満 |
| 1 | $10^{-6}$以上 $10^{-5}$未満 |

注)冗長化(多重化)による安全追求に頼らない、非冗長化構成

【(株)エム・システム技研　開発部】