

# シーケンス制御ソフトウェアにおけるセーフティの考え方

機械制御技術部 生産システムチーム 宮澤 以鋼

産業界においては安全に対する要求が強まりつつある。その傾向の一つとして、最終製品の安全性だけでなく、その製品の設計や製造における各プロセスでの安全性も求められていることがある。このための国際規格も整備され、多く発表されている。生産システムにおいても、ハードウェアの装置だけでなく、それに含まれているソフトウェアにも安全性を有する機能の概念が生まれ、セーフティシステムの認定にも必要不可欠の要素となっている。本稿では、シーケンス制御のソフトウェアにおけるセーフティの考え方について紹介し、PLCopenにおけるセーフティ機能性について説明する。

キーワード：PLC，セーフティ，セーフティ機能性，言語，セーフティファンクションブロック

## 1 はじめに

セーフティはセキュリティと並んで産業界における重要なキーワードの一つである。生産システムにおいても例外ではなく、製品そのものの安全性もさることながら、設計から製造まで各工程においてそれぞれの安全性が求められるのが近年のセーフティという概念の特徴である。さらに、製造装置などハードウェアの安全性と並んで、ソフトウェアにおける機能安全も重要であるという認識がコンセンサスとなりつつある。生産システムで制御装置として多く使用されているPLC (Programmable Logic Controller)においても、いわゆるセーフティPLCが誕生しており、セーフティコンポーネントを含めてセーフティシステムの構築に有力な道具となり得る。しかし、ハードウェアのセーフティよりもソフトウェアのセーフティの確立が遅れており、PLCopen (<http://www.plcopen.org/>) などの団体ではそのための規格整備を行っている。本稿では、PLCopenにおけるシーケンス制御ソフトウェアのセーフティの考え方について紹介する。

## 2 背景

近年では、安全に関する国際規格が急増している。電気関連分野においてIECとISOの主要なものとして、機能安全 (Functional Safety) と機械安全 (Machinery Safety) の二つの系列がある<sup>1)5)</sup>。機能安全はすべての電気関連機器を想定しており、機械安全はPLCを含めた機械装置が対象である。いずれにしてもPLCは安全系の構築においてその対象となる。

安全関連規格への対応は最終製品に求められており、製造メーカーが自製品に責任を持つので、小規模企業特に小さい機械メーカーにとってはその対応が困難で、コストの増大につながる。また、安全関連部分とこれを用いたアプリ

ケーション部分が分かれており、異なる環境やツールを使用して構築されたシステムや製造された製品の安全性の認定が常に問題となる。さらに、安全関連部分は最終段階で求められるため、初期の段階で考慮されているとは限らず、そのためのテストも不十分である可能性が高い。このため、PLCメーカーだけでなく、機械メーカーを含めた多くのPLCユーザがPLC関連セーフティの標準化を望んでいる。

## 3 セーフティ機能性

### 3.1 仕様作成とその目標

上述の背景において、産業界の要望を応えるためにPLCopenはPLCのソフトウェアのセーフティを確立すべく、PLCのセーフティ機能性について2003年6月からその仕様作成を始めた。正式リリース直前ではあるが、現在、その仕様がドラフトとして発表されている<sup>6)</sup>。

本仕様はシーケンス制御ソフトウェアのセーフティを確立するために作られているが、ハードウェアとの関係で、その優先順位を「機械関連第一、プロセス関連第二」と明確に定めてある。また、本仕様の目標として、セーフティ機能性を容易に使用できるインタフェースの提供を掲げており、既存のセーフティ規格との関連付けを明確にし、広範なアプリケーションに再利用可能な部分を取り上げる。その最終目標は、セーフティ機能性について異なるプラットフォーム間でのアプリケーションプログラムの再利用である。

さらに、将来的には、認証機関によって認可・承認された機能性や概念を共通化し標準化する。このように構築されたシステムによって共通のソフトウェア基盤を提供し、標準セーフティ機能性のための標準ファンクションブロック (FB: Function Block) のライブラリを構築し、参照のために流通させる。また、本仕様で定義されたものは将来FBの追加のためのフォーマットとなる。

### 3. 2 構造モデル

従来のシステムとセーフティシステムとの関係を図1の構造モデルで説明する。

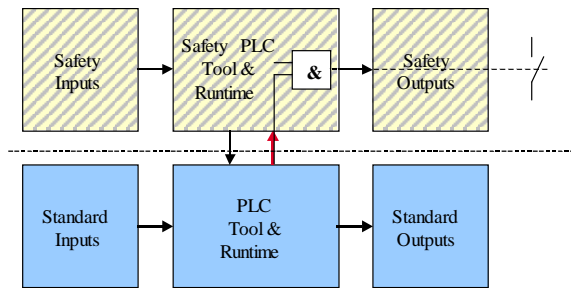


図1 構造モデル

真中の点線はシステムの境界線を示し、その上の部分は安全系 (Safety PLC) で下は非安全系 (PLC) である。安全系における入出力はセーフティコンポーネントが使用され、そのPLCはセーフティPLCである。非安全系のPLCと入出力はすべて従来のものである。

安全系と非安全系との間では信号のやり取りが可能で情報交換が行える。しかし、PLCopenの構造モデルによれば、安全系側の情報は非安全系側で無条件で参照できるのに対して、非安全系側の情報は安全系側での参照が条件付となっており、すなわち、条件付の参照はその情報の参照結果が安全であると保証される。

### 3. 3 三つのレベル

本仕様では、安全系を使用する者として三つのレベル、基本レベル (Basic level)、拡張レベル (Extended level)、システムレベル (System level) に分けた。

基本レベルは、指定されたFBを使用するセーフティアプリケーションのプログラマが対象となるレベルである。基本レベルでは、いわゆるプログラミング環境でセーフティFBを使用したアプリケーションの開発が想定されており、そのFBに対しての変更や拡張は認められていない。

拡張レベルは指定されたFBに対して特有の拡張の定義を可能にする拡張機能性レベルである。すなわち、セーフティFBに対して拡張が認められ、その新たに作られたFBも一定の規則のもとで新しいセーフティFBとして登録することも可能である。このレベルではシステム構築が想定されている。

最後のシステムレベルは指定されたFBの供給者による実装が対象となるレベルであるが、本仕様書の使用対象者外である。

### 3. 4 言語への制約

シーケンス制御ソフトウェアの構築は基本的に IEC 61131-3 PLC のプログラミング言語に基づく。このため、その安全性を実現する手段としても、IEC 61131-3の要素に制約を与え、使用できる言語要素を限定することによっ

て実現する。IEC 61131-3 で決められたものとしては、いわゆる 4 言語、IL (Instruction List)、ST (Structured Text)、FBD (Function Block Diagram) と LD (Ladder Diagram) 及び 1 共通要素、SFC (Sequential Function Chart) である。

安全系で好ましい言語としては図形言語の FBD と LD であり、その理由は一覧性に優れていることである。テキスト言語の IL と ST については現時点で議論しないとした。理由はテストや検証がより複雑でコスト高と考えられるためである。また、SFCはIEC 61131-3における定義が不十分という理由で使用すべきでないとしている。

### 3. 5 データ型への制約

データ型への制約は表1に示す。SAFEBOOLはIEC 61131-3にないデータ型で本仕様書において新たに追加されたものである。SAFEBOOLはソフトウェア上で実際に認識できるデータ型ではなく、セーフティコンポーネントの入出力を使用したとき、そのセーフティコンポーネントを表すために追加されたデータ型である。

表1 データ型への制約 (X:可, -:不可, 以下同)

Description	Basic Level	Extended Level
SAFEBOOL	X	X
BOOL	X	X
INT, DINT	X	X
REAL	X	X
WORD	X	X
TIME	X	X
Other ANY_BIT	-	-
Other ANY_INT	-	-
Other ANY_REAL	-	-
ANY_DATE	-	-
STRING	-	-

この表の制約から分かるように、データ型は基本的に大きく制約されている。Long型はないのはすべてのシステムで実装されているとは限らないという理由で、基本的なものだけに限定されている。総称型も実装における煩雑さを考えると、実装上のバグを避けるために除かれている。さらに、ユーザにとっては総称型でなく、ファンクションやFBの入出力に対して明確にデータ型を指定する必要があるため、勘違いによる使用者の間違いのリスクが軽減されると考えられる。

### 3. 6 変数の種類への制約

表2は変数の種類への制約である。許されているのは内部変数VAR、外部入力と出力変数VAR\_INPUTとVAR\_OUTPUT及び定数のCONSTANTである。

表2 変数の種類への制約

Description	Basic Level	Extended Level
VAR	X	X
VAR_INPUT/_OUTPUT	X	X
VAR_IN_OUT	-	-
VAR_GLOBAL/EXTERNAL	-	-
VAR_ACCESS	-	-
CONSTANT	X	X
RETAIN	-	-

ここでは特に入出力変数VAR\_IN\_OUTが使用すべきでないとされている。

### 3.7 標準ファンクションへの制約

基本レベルにおいては、ANDとOR以外のファンクションは使用できなくなっている。複雑な論理は安全でないとされている。拡張レベルでは論理演算における制約はほとんどないが、ビットシフトと実数の単項演算は両レベルにおいて共に制約されている。

表3 標準ファンクションへの制約

Description	Basic Level	Extended Level
AND, OR	X	X
XOR, NOT	-	X
ADD, MUL, SUB, DIV	-	X
SHL, SHR, ROR, ROL	-	-
GT, GE, EQ, LE, LT, NE	-	X
Selection functions	-	X
Type conversion functions	-	X
String functions	-	-
Time Functions	-	X
Unary REAL functions	-	-

### 3.8 標準FBへの制約

標準FBへの制約は表4に示す。基本レベルだけにおいて、双安定FBとエッジ検出FBの使用が制約されている。これらのFBは一般にシステムの実装に差があると思われる。

表4 標準FBへの制約

Description	Basic Level	Extended Level
TON, TOF, TP	X	X
CTU, CTD, CTUD	X	X
Bistable FB (SR, RS)	-	X
Edge Detection	-	X

### 3.9 その他の制約

その他の制約はまとめて表5に示す。さらに、Status messages, Error messages, Reset behaviorがある。

表5 その他の制約

Description	Basic Level	Extended Level
Definition of FB	X	X
Directly represented variables	-	-
STRUCT, ARRAY	-	-
LD, FBD	X	X
ST, SFC, IL	-	-
Other: C, C++, ...	-	-
EN / ENO in LD	-	-
Multiple call of same FB-instance	-	-
Feedback loop in same network	-	X
Multiple or Conditional Return	-	X
Jumps, Conditional Jumps	-	X
FB Declaration Features	-	-

図2のように、従来のFBにSFを付ければ安全FBとなる。

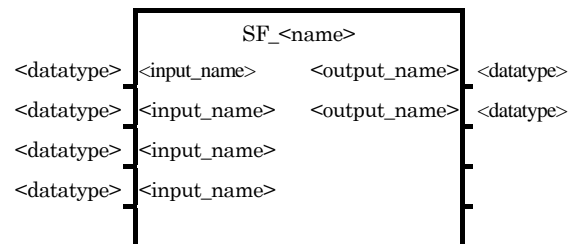


図2 安全FBの図式

## 4 おわりに

本稿で紹介されたセーフティ機能性は既に実装が試みられており、その成果に期待したい。

## 文献

- 1) IEC 61508, Functional safety of electrical/electronic/programmable electronic safety-related systems.
- 2) ISO 13849, Safety of machinery - Safety-related parts of control systems.
- 3) IEC 62061 (2005-01), Safety of machinery - Functional safety of safety-related electrical, electronic and programmable electronic control systems.
- 4) IEC 60204, Ed. 5.0 (2003-07), Safety of machinery - Electrical equipment of machines.
- 5) ISO 12100, Safety of machinery - Basic concepts, general principles for design.
- 6) PLCopen Technical Specification (2005-11), Safety Functionality - Part 1: Concepts and Function Blocks.