PLCopen最新技術動向

－PLCセーフティプログラミング－

PLCopen Japan

Safety-WG　深田 彰男

（株）東芝　電力流通・産業システム社

本日のお話

1. **Safe Softwareへの取組みの背景**
2. **PLCopenの取組みの紹介**
   - 2.1 技術仕様書／Safety Software - part 1: Concepts and Function Blocks
   - 2.2 技術仕様書／Safety Software - part 2: User Guidelines
   - 2.3 技術仕様書／Safety Software - part 3 ~ part 5 draft
3. **PLCopen Japan TC/Safety-WGの活動紹介**

Safe Softwareへの取組みの背景①

安全規格非関税障壁化の問題

Europe's 'Unity' Undoes a U.S. Exporter

By Timothy Aeppel
Staff Reporter of The Wall Street Journal

Economic unity may work for Europe, but it's a nightmare for some U.S. exporters.

As part of creating a single multinational market, European countries have forged common standards for everything from kidney-dialysis machines to food coloring. Many other items remain to be harmonized. However, when it comes to safety, the rules specifically allow countries to prohibit imports that threaten "public security."

That has made life miserable for Evan Segal. He is president of Dormont Manufacturing Co., which makes hoses that hook up deep-fat fryers and the like to gas outlets and which once sold these hoses freely throughout Europe. But one day in 1989, one of his top customers, Frymaster Corp. of Shreveport, La., called to alert him that McDonald's was being told it could no longer use his hoses in its British restaurants. Similar problems popped up elsewhere, including EuroDisney outside Paris; shortly before the theme park opened, French inspectors demanded that Dormont's hoses be replaced with French-approved equipment.

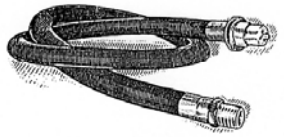
The disparate national standards stemmed from the fact that hoses are crucial to the safe operation of gas appliances and thus fall under the product-safety provisions allowing each country to set up its own standards. But as he studied the rules, Mr. Segal realized he would never be able to meet them.

"My competitors basically wrote the rules to describe their own products," says Mr. Segal, whose company is based, ironically, in Export, Pa., and has annual sales of $25 million.

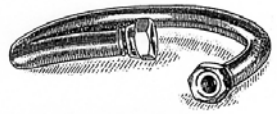
Some big U.S. multinationals with longstanding European ties have benefited from the Europeans' move to forge common standards, and other U.S. exporters are largely unaffected. However, U.S. trade officials estimate that at least $300 million of the $112 billion in U.S. exports to Europe are goods that once needed no separate national approvals but now require such approval from each country.

In Dormont's case, the specifications were written by committees often dominated by domestic producers. They spell out minutiae of each country's acceptable gas-hose design—such as the color of plastic coating or how the end pieces should be attached to the rest of the hose. All designs are unlike Mr. Segal's own brand of hoses, and he argues that there is no logic to the differences in design "other than that it makes it easier for them to push people like me out of their markets." (In the U.S., standards for hoses are based on performance and safety, rather than the details of design.)

DORMONT'S GAS HOSE
- Stainless-steel helical tubing (molded from continuous spiral)
- Flare-type seals at ends
- No covering



BRITISH HOSE REQUIREMENTS
- Galvanized metal annular tubing (made of metal formed into concentric circles)
- Set length, can't be extendable
- Rubber covering



ITALIAN HOSE REQUIREMENTS
- Stainless steel annular tubing
- Must be extendable
- No covering

The Dormont case "is clearly a case of European standards being used as a technical barrier to trade," says Sergio Mazza, president of the American National Standards Institute, an organization that works to harmonize standards.

Rene Van De Zande, a U.S. Commerce Department official based in Brussels who has followed the Dormont case closely, agrees the rules are unfair. "It seems that there are national competitors of Dormont in [Europe] that want to keep out Dormont," he says.

Trade and commerce officials in the U.S. agree. "We've gone to bat in a major way for this company—because we do think they are being treated unfairly," says one. Both U.S. Trade Rep. Mickey Kantor and Commerce Secretary Ron Brown have cited the European penchant for design-based standards as a potential hindrance for exporters.

Mr. Segal thought he had made a major breakthrough in 1993, when the British Standards Institute, one of the European agencies that test equipment and hand out approvals, issued Dormont a certificate authorizing the company to paste a seal of approval on its products signifying that the hoses conformed with European Union rules for gas appliances—thus enabling the company to sell them throughout the region.

But the victory was short-lived. A miffed German competitor fired off a formal complaint to the European Commission, the EU's Brussels-based executive body. Commission officials familiar with the case say the rival argued that the British office erred because hoses are not really part of a gas appliance. The approval was withdrawn.

Joseph Putzeys, head of the commission office that reviewed the case, defends the rejection of Mr. Segal's product. He says the trouble is the threaded fittings at the ends of the hoses that connect them to gas lines. These threadings vary from country to country. "If it's not compatible," he says, "you may have gas leaks."

Dormont hoses have gone through rigorous approval processes in both the U.S. and Canada, and Mr. Segal notes that while threadings may vary, hoses can easily accommodate the variations with inexpensive adapters.

The U.S. is now pressing Britain to redraft its rules to ax design specifications. British officials say that the nation's product standards are voluntary, but most gas installers in Britain refuse to handle equipment that lacks the voluntary approval.

Elsewhere in Europe, there are signs Dormont is making inroads. Belgium recently gave the company approval to sell in that small country, and Dormont is now working on Denmark. Mr. Segal hopes individual approvals will strengthen his case for Europewide recognition.

—James Pressley contributed to this article.

同じ安全性を目指しながら、
国によって異なる仕様

- Dormont's Gas Hose
  - Stainless-steel helical tubing (molded from continuous spiral)
  - Flare-type seals at ends
  - No covering
- British Hose Requirements
  - Galvanized metal annular tubing (made of metal formed into concentric circles)
  - Set length, can't be extendable
  - Rubber covering
- Italian Hose Requirements
  - Stainless steel annular tubing
  - Must be extendable
  - No covering

Wallstreet Journal 4/1/1996掲載の記事

機能安全標準化の必要性

- 各種安全規格の整合化が必要。
  - ISO/IEC Guide 51 (1990)-G 51
  - ISO/IEC Guide 51 (1999)-G 51 E（改訂第2版）
  - G 51-Eでは、基本安全規格、グループ安全規格、製品安全規格に分類。
  - IEC 61508はG 51に基づく最初の基本安全規格。
- 安全機能遂行に当たって従来のハードウェアでの制御だけでなく、複雑化する安全制御に対応するために新たにソフトウェアでの制御技術が不可欠となり、これへの対応（ガイドライン作成）が必要。

Safe Softwareへの取組みの背景③

■ 機能安全関連規格の動向（各種安全規格間の整合と個別規格への展開）

IEC 61508（JIS C 0508）
電気・電子・プログラマブル電子機器（E/E/PE）安全関連系の機能安全
（Ed.2 CDV文書可決）

機能安全対応
ISOの改正

ISO/EN 13849-1（JIS B 9705-1）
機械制御システムの安全部設計のための一般原則（2006改訂版発行、JIS改正中）

IEC分野別
共通規格

IEC個別製品規格化

IEC 61800（2007制定）
可変速電気駆動システム（PDS=INV, SV）
安全要求事項
IEC 61800-5-1:電気、発熱、エネルギー
IEC 61800-5-2:機能安全

IEC62061
機械の安全性－安全関連の電気・電子・プログラマブル電子制御システムの機能安全

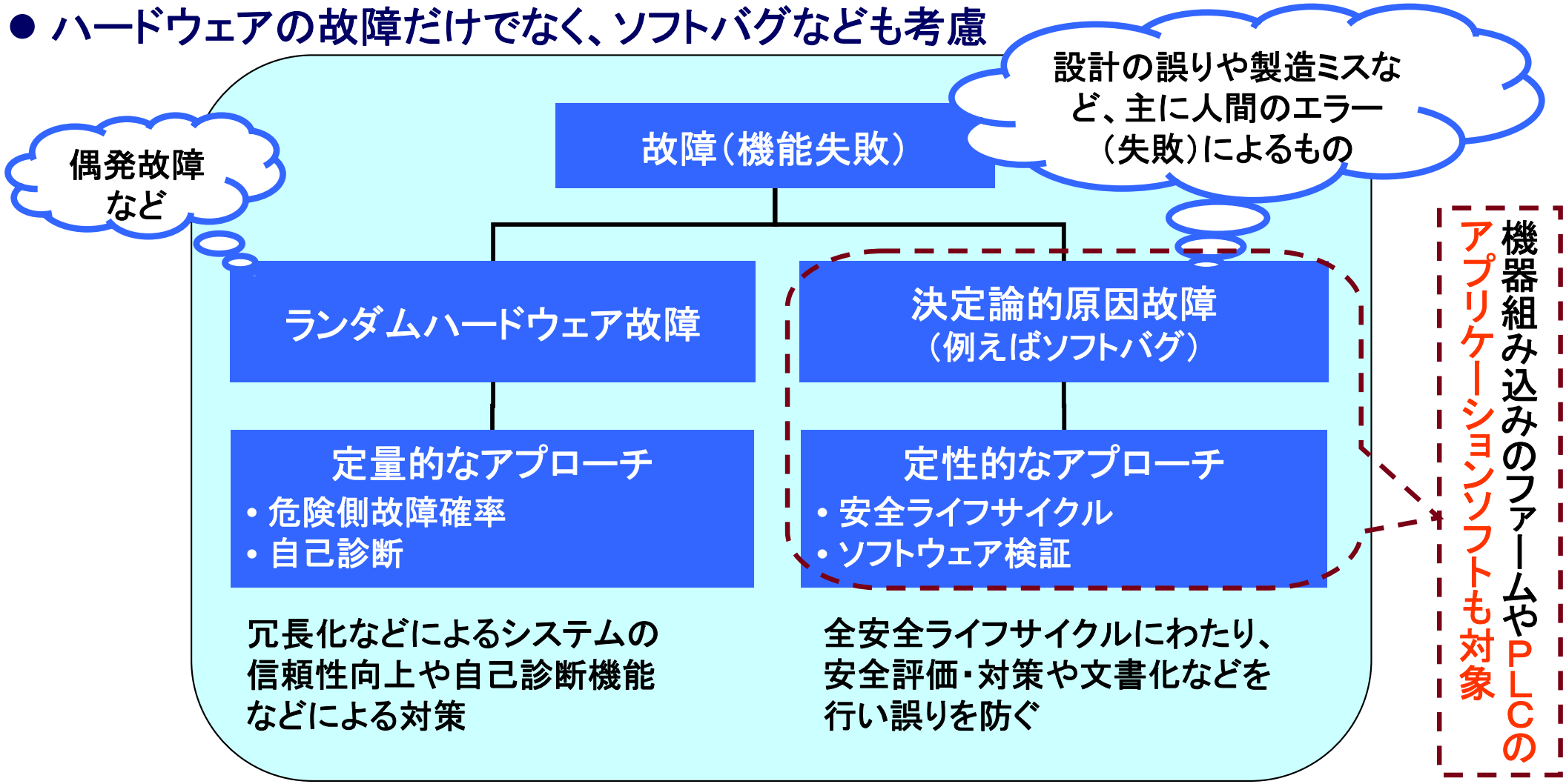
IEC61511
（JIS C 0511）
プロセス産業のための計測制御システムの機能安全

IEC 61131-6
プログラマブルコントローラの機能安全
＝FS PLC（CD文書審議中）

Safe Softwareへの取組みの背景④

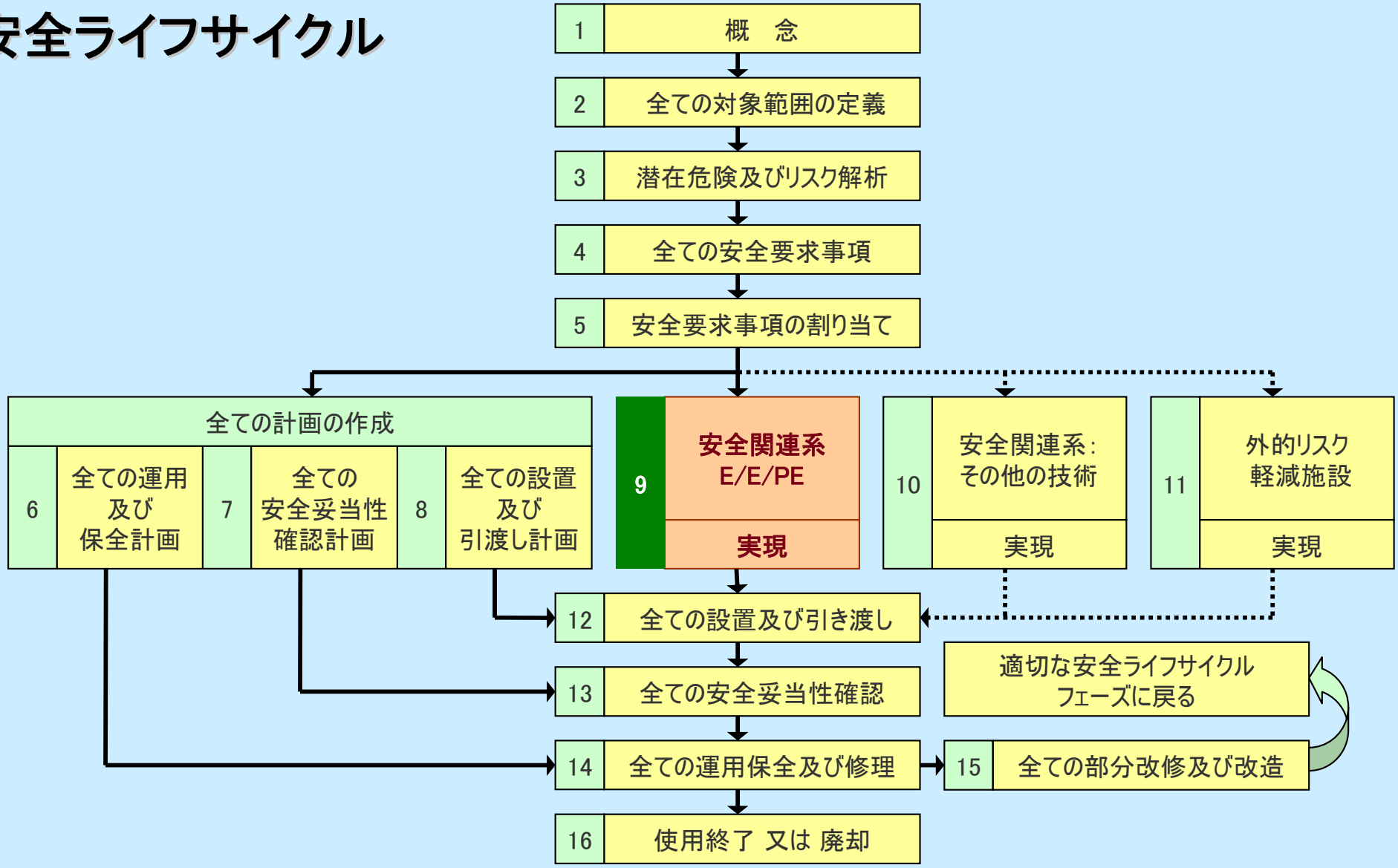
■ 規格IEC 61508の概念

- 安全度水準SIL 1～4を規定
- ハードウェアの故障だけでなく、ソフトバグなども考慮



Safe Softwareへの取組みの背景⑤

安全ライフサイクル



PLCopenの取組み

- アプリケーションソフトの安全確保

- 技術仕様書Safety Software part 1, part 2の発行
  - Part 1: Concepts and Function Blocks　2006/01 V1.0発行
  - Part 2: User Guidelines　2008/02 V1.0発行, 2008/07 V1.01改訂


PLCopen
for efficiency in automation

PLCopen - Technical Committee 5
–
Safety Software

Technical Specification

Part 1: Concepts and Function Blocks

Version 1.0 – Official Release

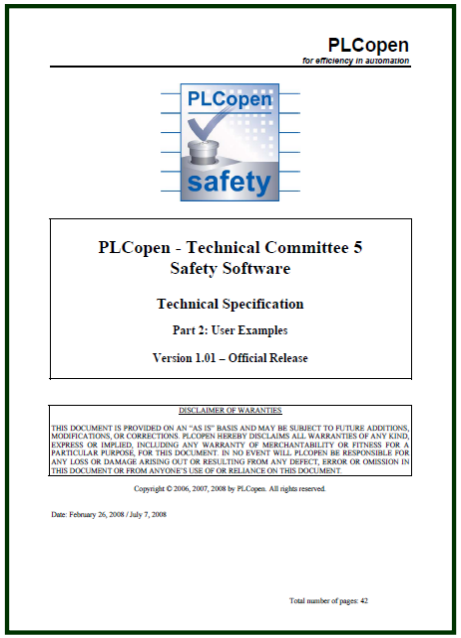
DISCLAIMER OF WARRANTIES

THIS DOCUMENT IS PROVIDED ON AN "AS IS" BASIS AND MAY BE SUBJECT TO FUTURE ADDITIONS, MODIFICATIONS OR CORRECTIONS. PLCOPEN HEREBY DISCLAIMS ALL WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING ANY WARRANTY OF MERCHANTABILITY OR SUITABILITY FOR A PARTICULAR PURPOSE. FOR THIS DOCUMENT UNDER NO CIRCUMSTANCES WILL PLCOPEN BE RESPONSIBLE FOR ANY LOSS OR DAMAGE ARISING OR RESULTING FROM ANY DEFECT, ERROR OR OMISSION IN THIS DOCUMENT OR FROM ANY USE OF OR RELIANCE ON THIS DOCUMENT.

Copyright © 2003 - 2006 by PLCopen. All rights reserved.

Date: Jan. 31, 2006.

Total number of pages: 149


PLCopen
for efficiency in automation

PLCopen - Technical Committee 5
Safety Software

Technical Specification

Part 2: User Examples

Version 1.01 – Official Release

DISCLAIMER OF WARANTIES

THIS DOCUMENT IS PROVIDED ON AN "AS IS" BASIS AND MAY BE SUBJECT TO FUTURE ADDITIONS, MODIFICATIONS, OR CORRECTIONS. PLCOPEN HEREBY DISCLAIMS ALL WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. FOR THIS DOCUMENT. IN NO EVENT WILL PLCOPEN BE RESPONSIBLE FOR ANY LOSS OR DAMAGE ARISING OUT OR RESULTING FROM ANY DEFECT, ERROR OR OMISSION IN THIS DOCUMENT OR FROM ANYONE'S USE OF OR RELIANCE ON THIS DOCUMENT.

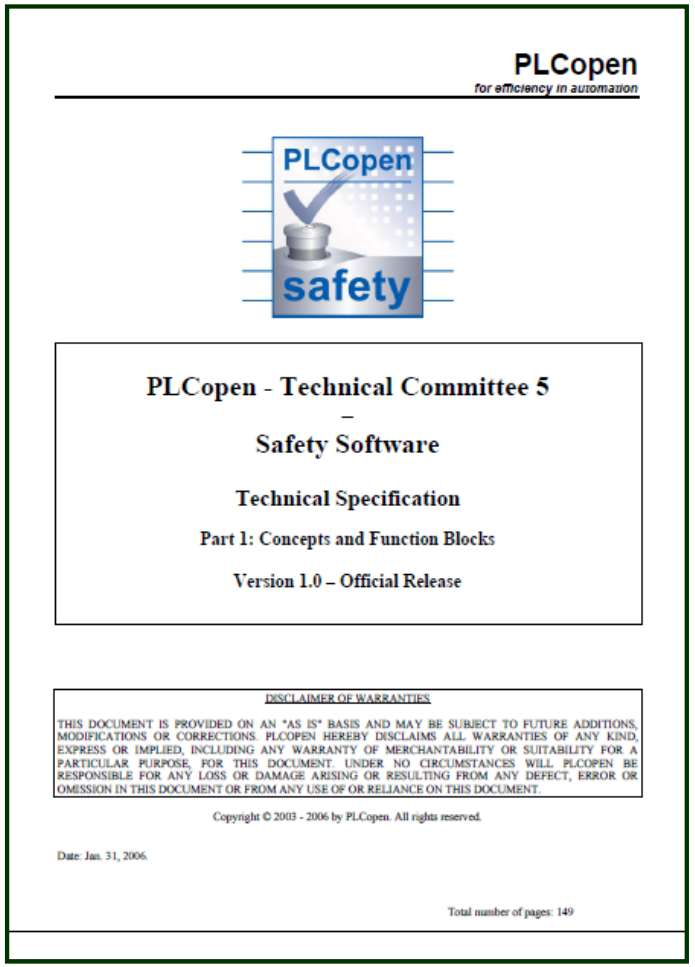
Copyright © 2006, 2007, 2008 by PLCopen. All rights reserved.

Date: February 26, 2008 / July 7, 2008

Total number of pages: 42

技術仕様書パート1の要点

- ソフトウェア構築手法の解説
- プログラミング言語の定義
- データ型の定義
- 言語サブセットの定義
- 安全・迅速なソフト作成、ユーザレベル定義
- エラー処理および診断コンセプトの提示
- 20のファンクションブロック(FB)の定義
- FB認証ガイドラインの提示



PLCopen
for efficiency in automation

PLCopen - Technical Committee 5
–
Safety Software

Technical Specification

Part 1: Concepts and Function Blocks

Version 1.0 – Official Release

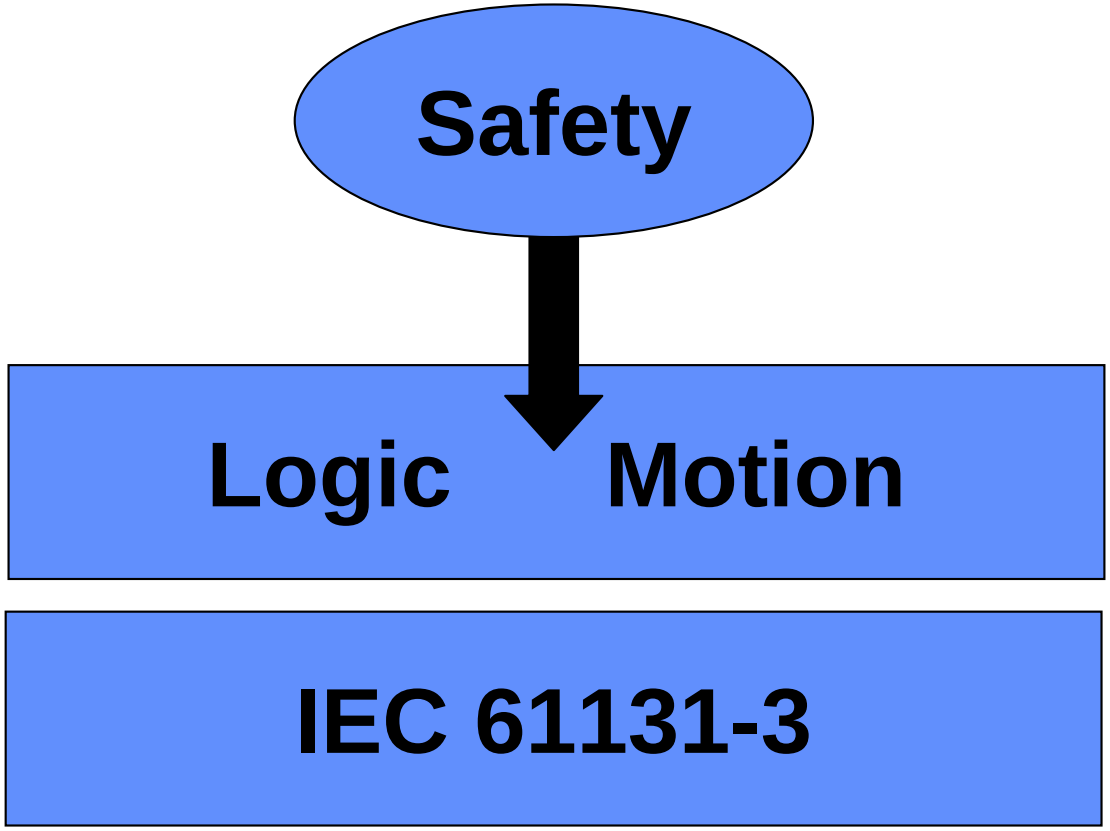
DISCLAIMER OF WARRANTIES

THIS DOCUMENT IS PROVIDED ON AN "AS IS" BASIS AND MAY BE SUBJECT TO FUTURE ADDITIONS, MODIFICATIONS OR CORRECTIONS. PLCOPEN HEREBY DISCLAIMS ALL WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING ANY WARRANTY OF MERCHANTABILITY OR SUITABILITY FOR A PARTICULAR PURPOSE, FOR THIS DOCUMENT. UNDER NO CIRCUMSTANCES WILL PLCOPEN BE RESPONSIBLE FOR ANY LOSS OR DAMAGE ARISING OR RESULTING FROM ANY DEFECT, ERROR OR OMISSION IN THIS DOCUMENT OR FROM ANY USE OF OR RELIANCE ON THIS DOCUMENT.

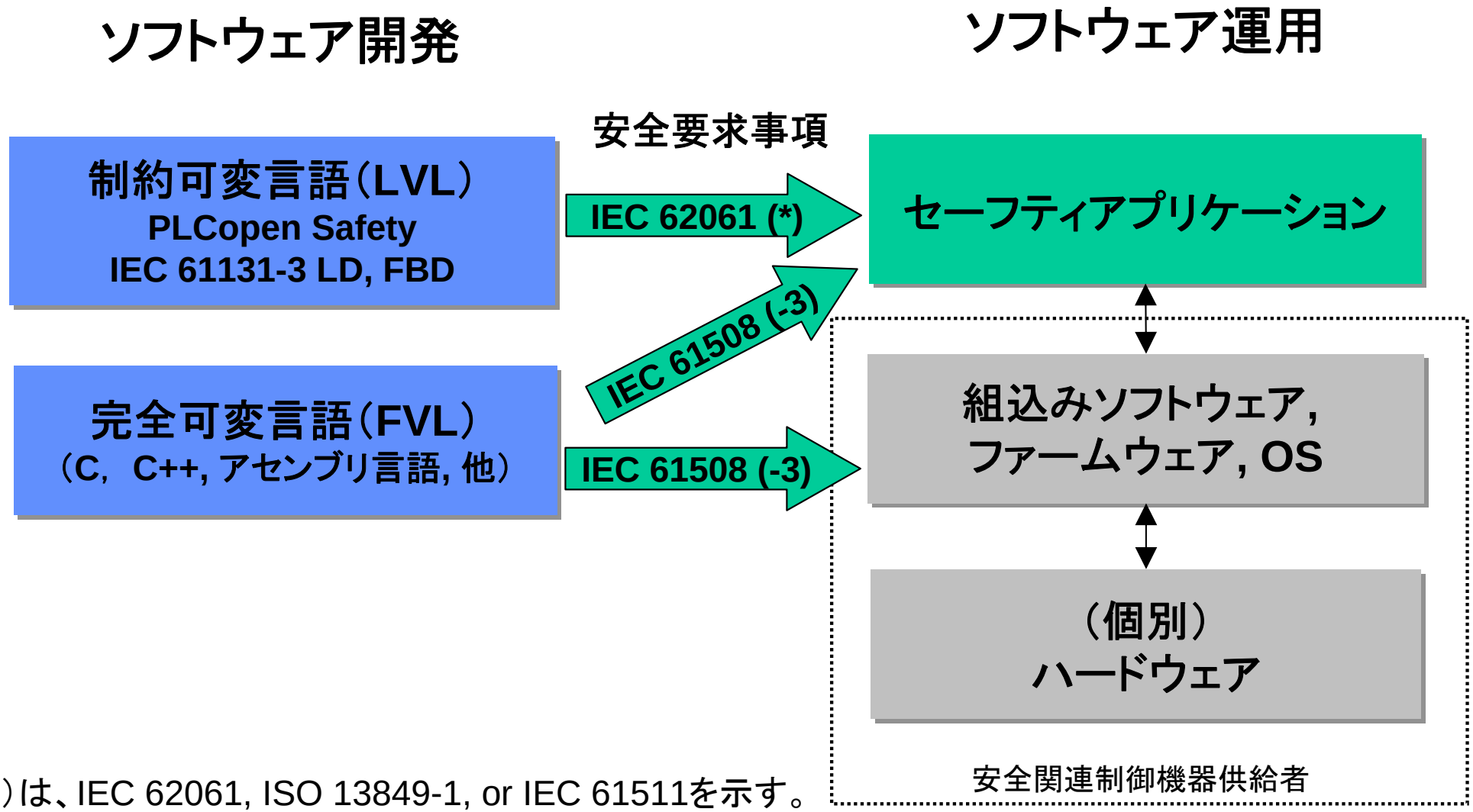
Date: Jan. 31, 2006.

Total number of pages: 149

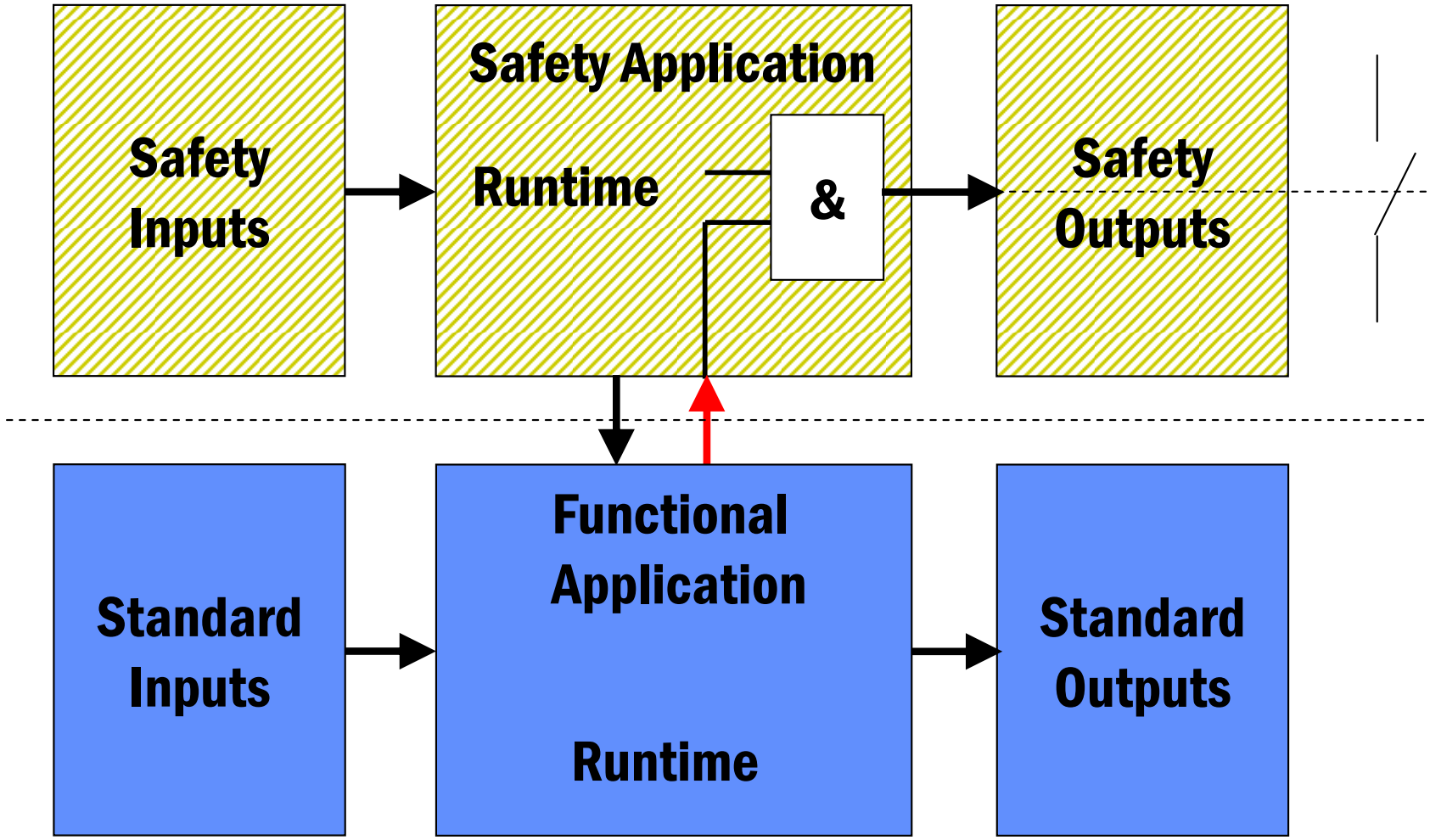
安全の統合



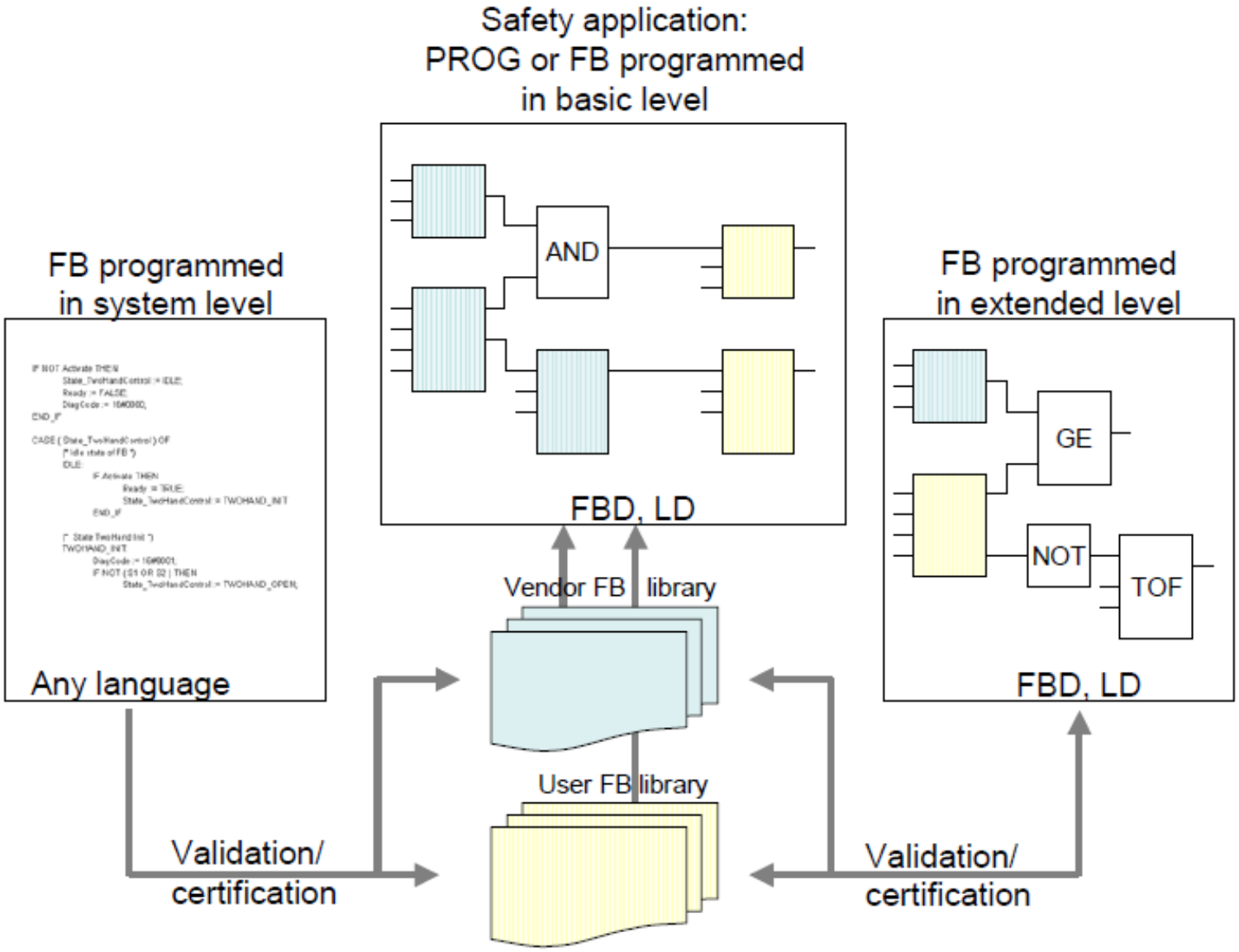
パート1-2　開発フェーズ、運用フェーズ 適用される規格の関係

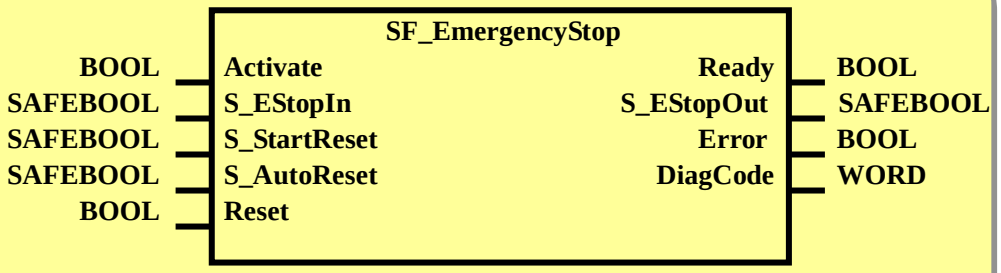


（*）は、IEC 62061, ISO 13849-1, or IEC 61511を示す。

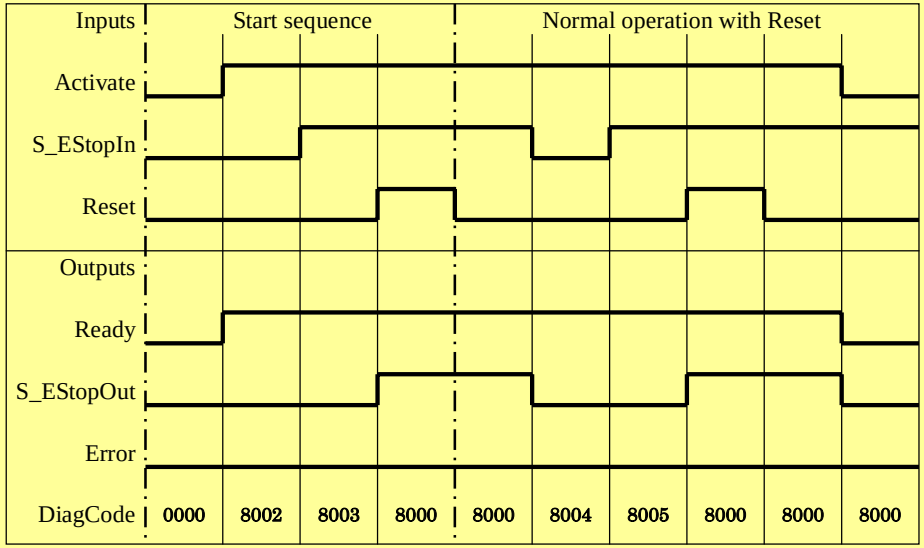

Safety
Inputs
Safety Application
Runtime
&
Safety
Outputs
Standard
Inputs
Functional
Application
Runtime
Standard
Outputs

パート1-4　各レベルに対する推奨適用スコープ

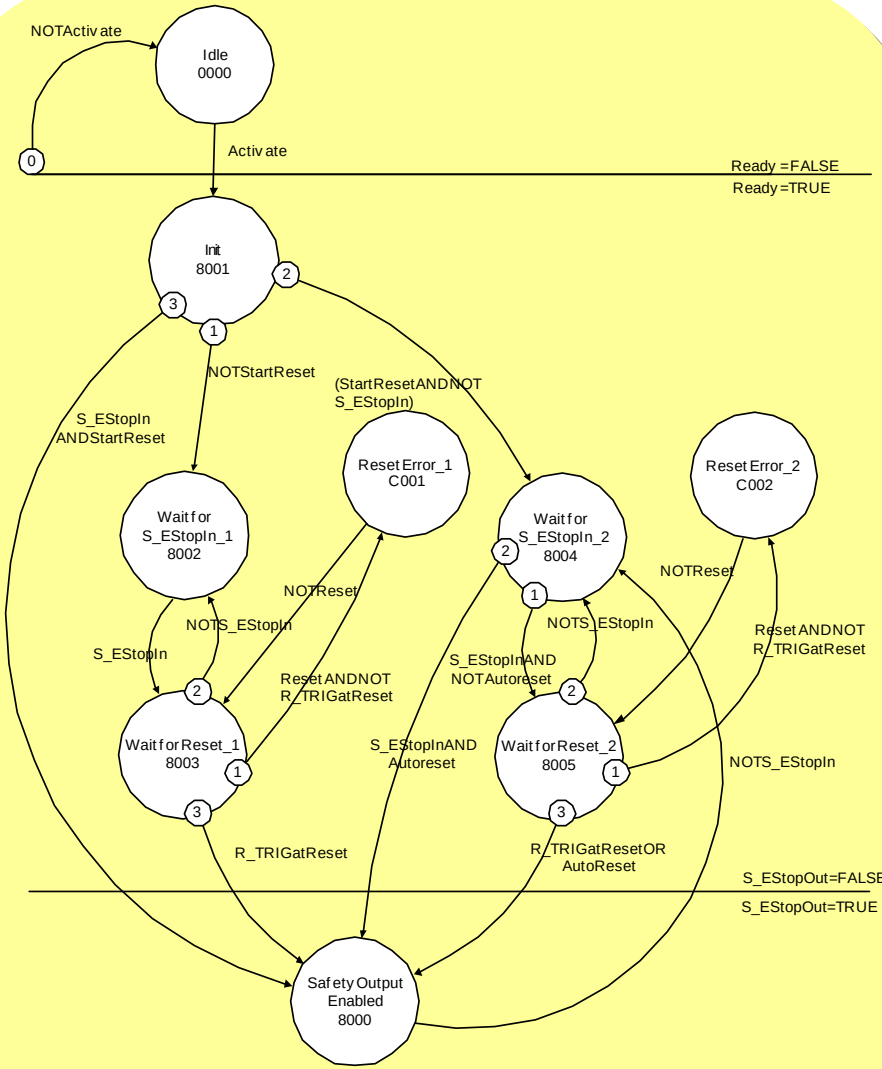




FBシンボル



タイミングチャート



状態遷移図

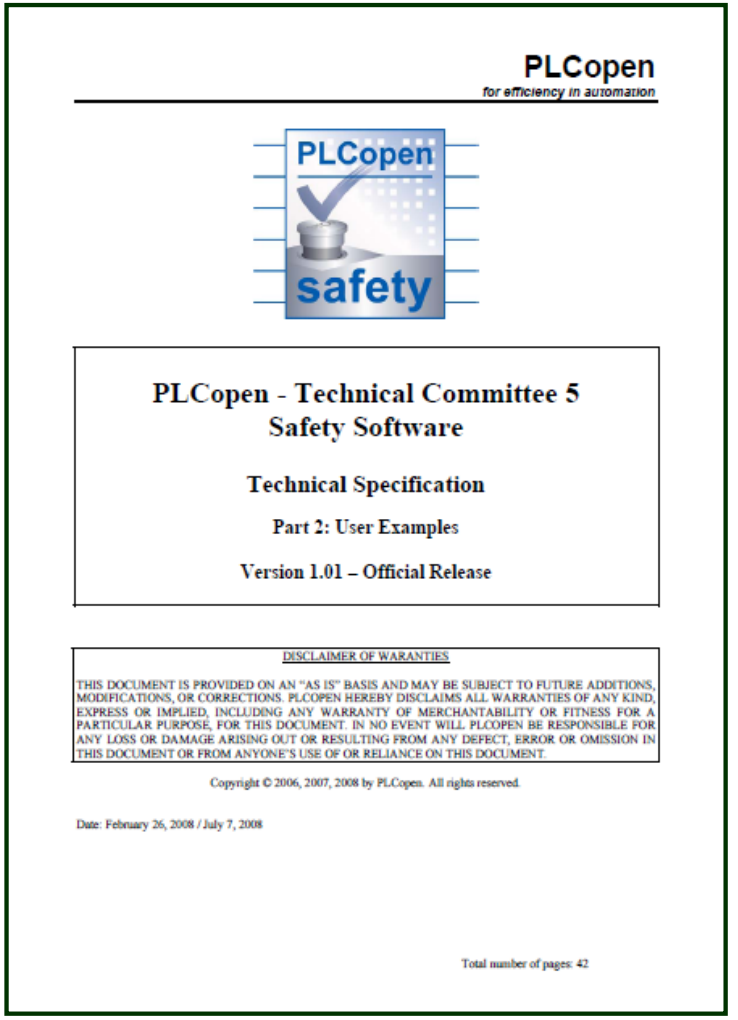
技術仕様書パート2

構成

1. Introduction
2. General Overview

   安全計画の策定、用語の定義、
   製造ラインにおける安全機能の例、
   PLCopen FBの適用
3. General Notes

   PLCopen FBと周辺との接続、
   セーフティアプリケーション例のグラフィカルオーバビュー
   に関する情報、セーフドライブの使用に関する情報
4. Application Examples



PLCopen
for efficiency in automation

PLCopen - Technical Committee 5
Safety Software

Technical Specification

Part 2: User Examples

Version 1.01 – Official Release

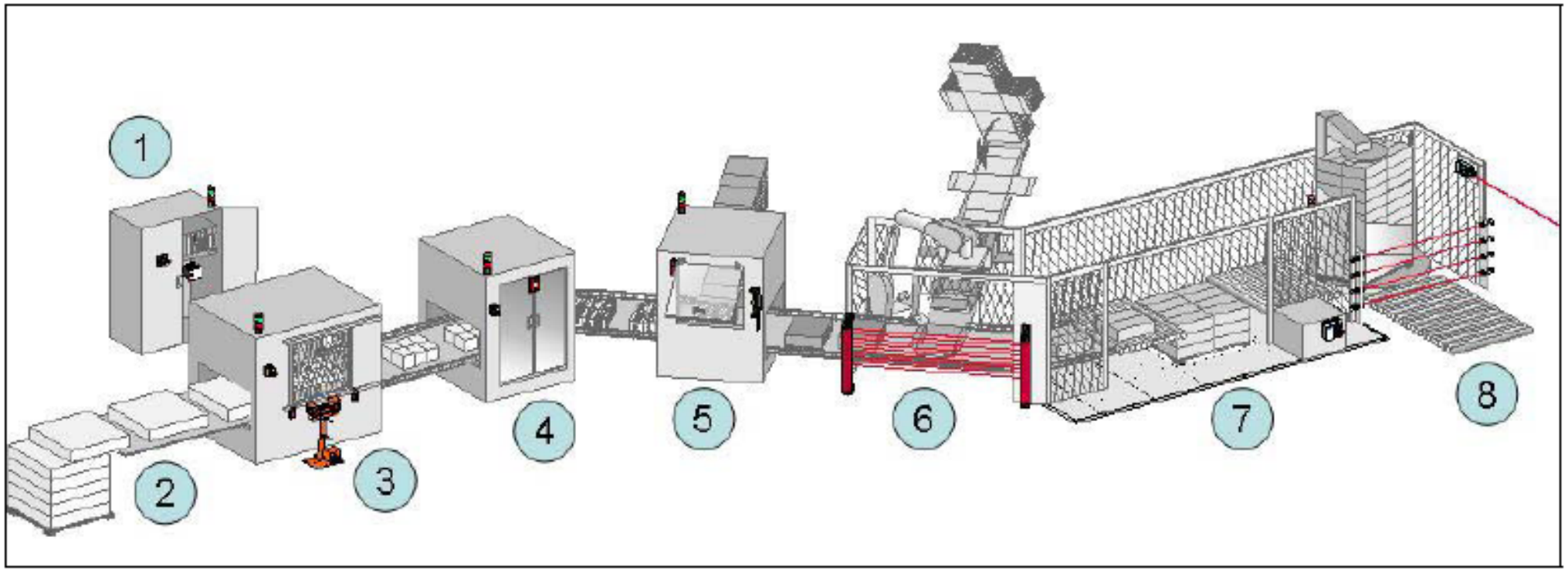
DISCLAIMER OF WARANTIES

THIS DOCUMENT IS PROVIDED ON AN "AS IS" BASIS AND MAY BE SUBJECT TO FUTURE ADDITIONS, MODIFICATIONS, OR CORRECTIONS. PLCOPEN HEREBY DISCLAIMS ALL WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, FOR THIS DOCUMENT. IN NO EVENT WILL PLCOPEN BE RESPONSIBLE FOR ANY LOSS OR DAMAGE ARISING OUT OR RESULTING FROM ANY DEFECT, ERROR OR OMISSION IN THIS DOCUMENT OR FROM ANYONE'S USE OF OR RELIANCE ON THIS DOCUMENT.

Date: February 26, 2008 / July 7, 2008

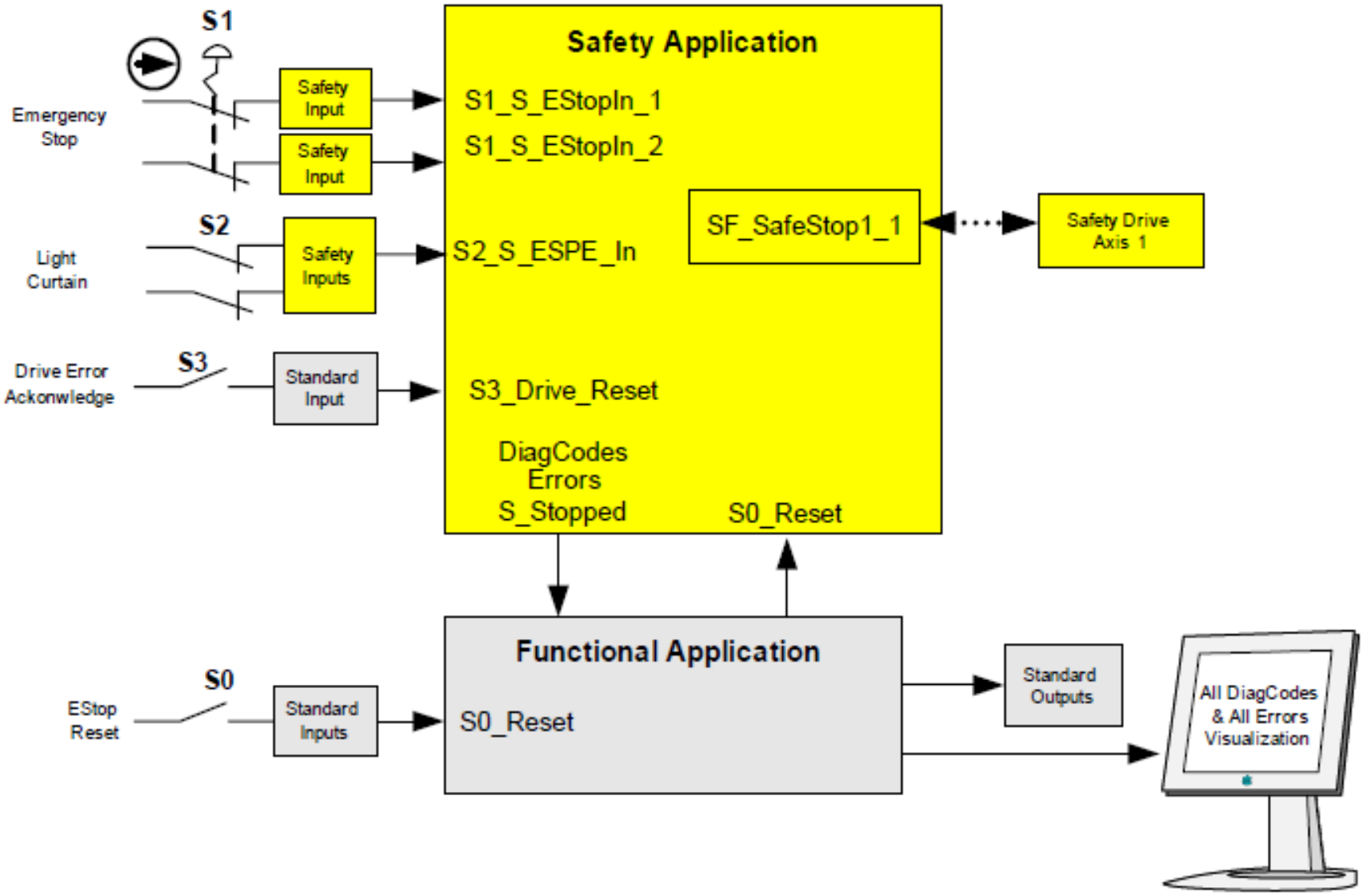
Total number of pages: 42

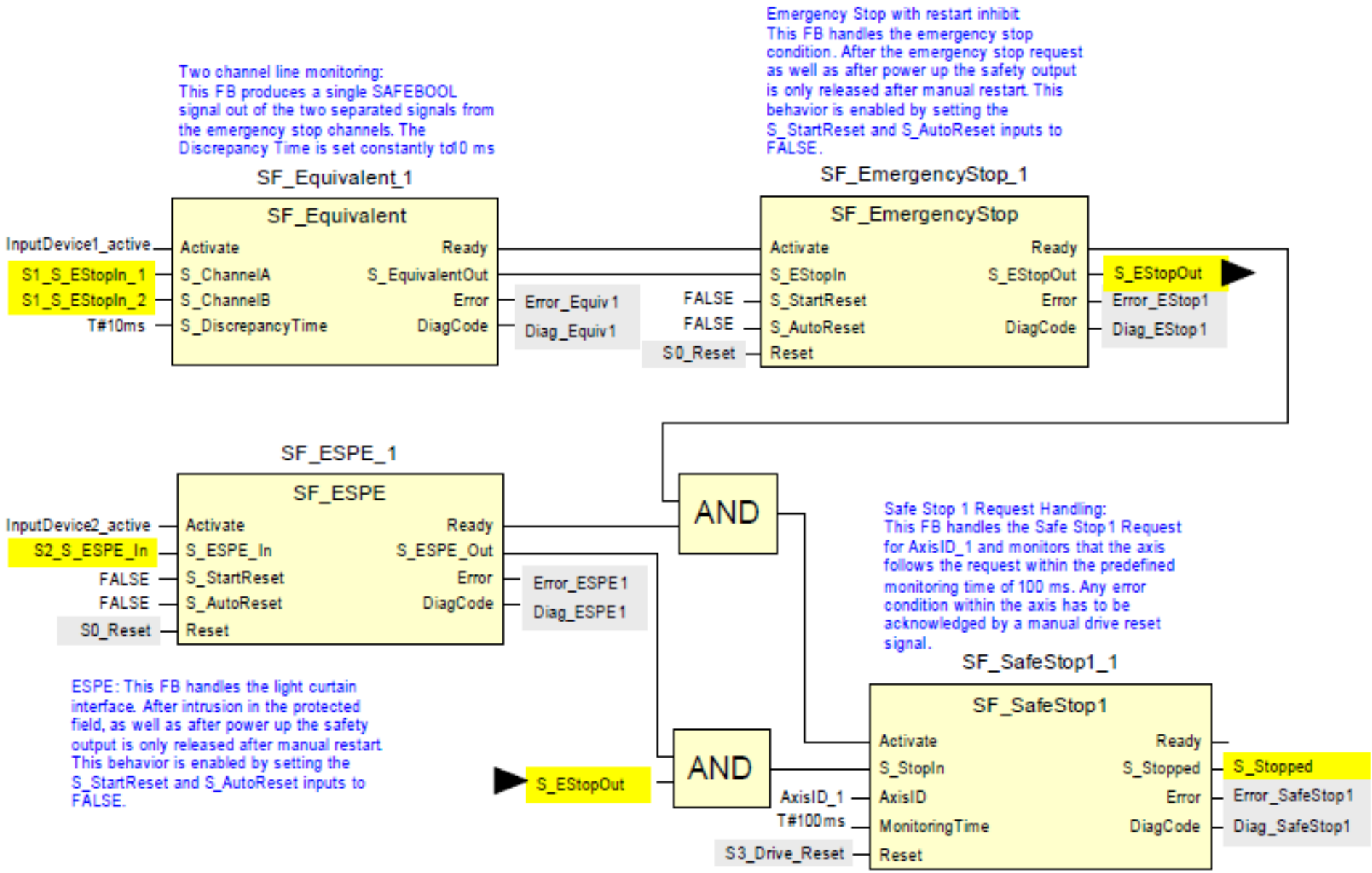
パート2-1 安全機能を組込んだ製造ラインの例



① 中央制御キャビネット（安全関連FB稼働中）
② 材料の供給点（この例では安全関連機能なし）
③ 材料の切断装置
（ドアモニタリングシステム付きの両手による安全機能）
④ 自動印刷装置（ドアモニタリングによる安全機能）
⑤ 一次梱包装置（ドアモニタリングによる安全機能）
⑥ 二次梱包装置（防護装置によるガードつき）
⑦ パレット組込み装置（安全マットによるガードつき）
⑧ 包装装置
（生産ラインの終点／ライトビームによる安全装置）

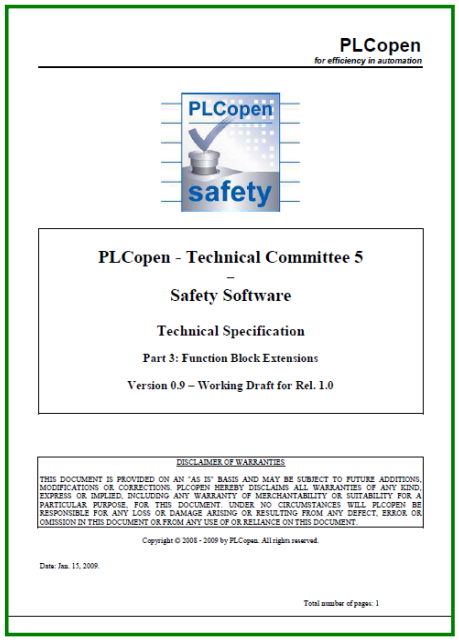
- 上記例では15種の安全FBが稼働している。

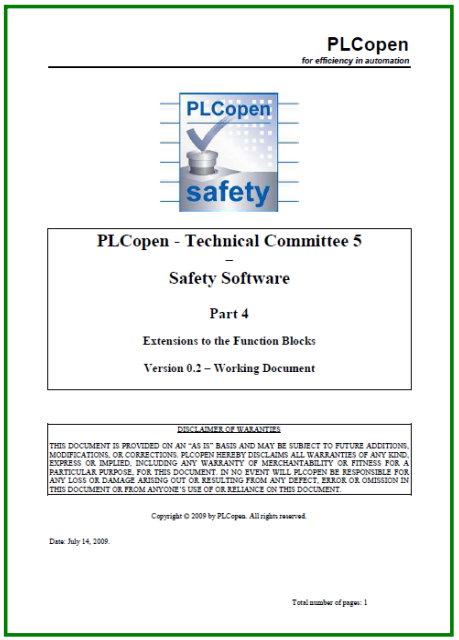

S1
Emergency Stop
Safety Input
Safety Input
S2
Light Curtain
Safety Inputs
Drive Error Ackonwledge
S3
Standard Input
S0
EStop Reset
Standard Inputs
Safety Application
S1_S_EStopIn_1
S1_S_EStopIn_2
S2_S_ESPE_In
SF_SafeStop1_1
Safety Drive Axis 1
S3_Drive_Reset
DiagCodes
Errors
S_Stopped
S0_Reset
Functional Application
S0_Reset
Standard Outputs
All DiagCodes & All Errors Visualization

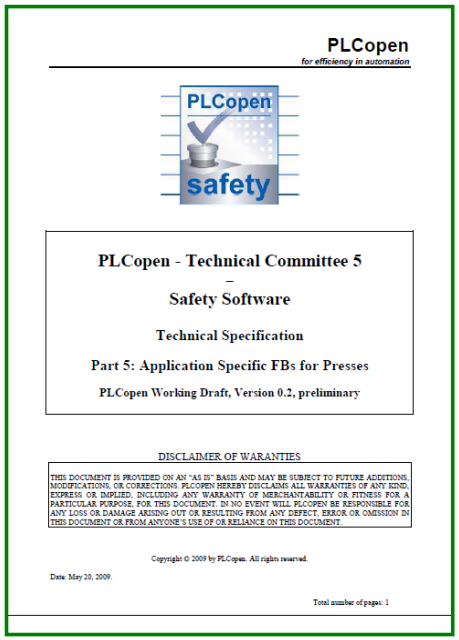

Two channel line monitoring:
This FB produces a single SAFEBOOL signal out of the two separated signals from the emergency stop channels. The Discrepancy Time is set constantly to10 ms
SF_Equivalent_1
SF_Equivalent
InputDevice1_active
S1_S_EStopIn_1
S1_S_EStopIn_2
T#10ms
Activate
S_ChannelA
S_ChannelB
S_DiscrepancyTime
Ready
S_EquivalentOut
Error
DiagCode
Error_Equiv1
Diag_Equiv1
Emergency Stop with restart inhibit
This FB handles the emergency stop condition. After the emergency stop request as well as after power up the safety output is only released after manual restart. This behavior is enabled by setting the S_StartReset and S_AutoReset inputs to FALSE.
SF_EmergencyStop_1
SF_EmergencyStop
FALSE
FALSE
S0_Reset
Activate
S_EStopIn
S_StartReset
S_AutoReset
Reset
Ready
S_EStopOut
Error
DiagCode
S_EStopOut
Error_EStop1
Diag_EStop1
SF_ESPE_1
SF_ESPE
InputDevice2_active
S2_S_ESPE_In
FALSE
FALSE
S0_Reset
Activate
S_ESPE_In
S_StartReset
S_AutoReset
Reset
Ready
S_ESPE_Out
Error
DiagCode
Error_ESPE1
Diag_ESPE1
AND
AND
ESPE: This FB handles the light curtain interface. After intrusion in the protected field, as well as after power up the safety output is only released after manual restart. This behavior is enabled by setting the S_StartReset and S_AutoReset inputs to FALSE.
S_EStopOut
Safe Stop 1 Request Handling:
This FB handles the Safe Stop 1 Request for AxisID_1 and monitors that the axis follows the request within the predefined monitoring time of 100 ms. Any error condition within the axis has to be acknowledged by a manual drive reset signal.
SF_SafeStop1_1
SF_SafeStop1
AxisID_1
T#100ms
S3_Drive_Reset
Activate
S_StopIn
AxisID
MonitoringTime
Reset
Ready
S_Stopped
Error
DiagCode
S_Stopped
Error_SafeStop1
Diag_SafeStop1

PLCopenの取組み

- **技術仕様書Safety Software part 3 ~ part 5のドラフト**
  - Part 3: Function Block Extensions　2008/01 V0.9 / Working Draft発行
  - Part 4: Extensions to the Function Blocks
    2008/07 V0.2 / Working Draft改訂
  - Part 5: Application Specific FBs for Presses
    2009/05 V0.2 / Working Draft改訂


PLCopen
for efficiency in automation
PLCopen - Technical Committee 5
–
Safety Software
Technical Specification
Part 3: Function Block Extensions
Version 0.9 – Working Draft for Rel. 1.0
DISCLAIMER OF WARRANTIES
THIS DOCUMENT IS PROVIDED ON AN "AS IS" BASIS AND MAY BE SUBJECT TO FUTURE ADDITIONS, MODIFICATIONS, OR CORRECTIONS. PLCOPEN HEREBY DISCLAIMS ALL WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING ANY WARRANTY OF MERCHANTABILITY OR SUITABILITY FOR A PARTICULAR PURPOSE. FOR THIS DOCUMENT, UNDER NO CIRCUMSTANCES WILL PLCOPEN BE RESPONSIBLE FOR ANY LOSS OR DAMAGE ARISING OR RESULTING FROM ANY DEFECT, ERROR OR OMISSION IN THIS DOCUMENT OR FROM ANY USE OF OR RELIANCE ON THIS DOCUMENT.
Copyright © 2008 - 2009 by PLCopen. All rights reserved.
Date: Jan. 15, 2009.
Total number of pages: 1


PLCopen
for efficiency in automation
PLCopen - Technical Committee 5
–
Safety Software
Part 4
Extensions to the Function Blocks
Version 0.2 – Working Document
DISCLAIMER OF WARRANTIES
THIS DOCUMENT IS PROVIDED ON AN "AS IS" BASIS AND MAY BE SUBJECT TO FUTURE ADDITIONS, MODIFICATIONS, OR CORRECTIONS. PLCOPEN HEREBY DISCLAIMS ALL WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. FOR THIS DOCUMENT, IN NO EVENT WILL PLCOPEN BE RESPONSIBLE FOR ANY LOSS OR DAMAGE ARISING OUT OR RESULTING FROM ANY DEFECT, ERROR OR OMISSION IN THIS DOCUMENT OR FROM ANYONE'S USE OF OR RELIANCE ON THIS DOCUMENT.
Copyright © 2009 by PLCopen. All rights reserved.
Date: July 14, 2009.
Total number of pages: 1


PLCopen
for efficiency in automation
PLCopen - Technical Committee 5
–
Safety Software
Technical Specification
Part 5: Application Specific FBs for Presses
PLCopen Working Draft, Version 0.2, preliminary
DISCLAIMER OF WARANTIES
THIS DOCUMENT IS PROVIDED ON AN "AS IS" BASIS AND MAY BE SUBJECT TO FUTURE ADDITIONS, MODIFICATIONS, OR CORRECTIONS. PLCOPEN HEREBY DISCLAIMS ALL WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. FOR THIS DOCUMENT, IN NO EVENT WILL PLCOPEN BE RESPONSIBLE FOR ANY LOSS OR DAMAGE ARISING OUT OR RESULTING FROM ANY DEFECT, ERROR OR OMISSION IN THIS DOCUMENT OR FROM ANYONE'S USE OF OR RELIANCE ON THIS DOCUMENT.
Copyright © 2009 by PLCopen. All rights reserved.
Date: May 20, 2009.
Total number of pages: 1

2007/10より「Safety-WG」として正式に活動開始。

- **活動目的**
  - IEC 61131-3環境における安全プログラム標準化に関する調査・研究
  - PLCopen TC5:Safetyの活動情報の収集、分析、課題の抽出。
  - PLCopen Japanとしての意見集約、PLCopen TC5/Safetyへの提案。
- **今年度の主たる活動**
  - 技術仕様書Safety Software / Part 1の日本語版発行。

PLCopen Japan Safety-WGでは、パート1和文版制作に取組み、年内をメドに発行の予定です。

- **WGメンバ**
  - 2009年10月現在、4社6名が参加。
    神奈川県産業技術センター、(株)キーエンス、富士電機システムズ(株)、(株)東芝
  - ベンダ会員、エグゼクティブ会員になれば誰でも参加可能。

ご清聴ありがとうございました