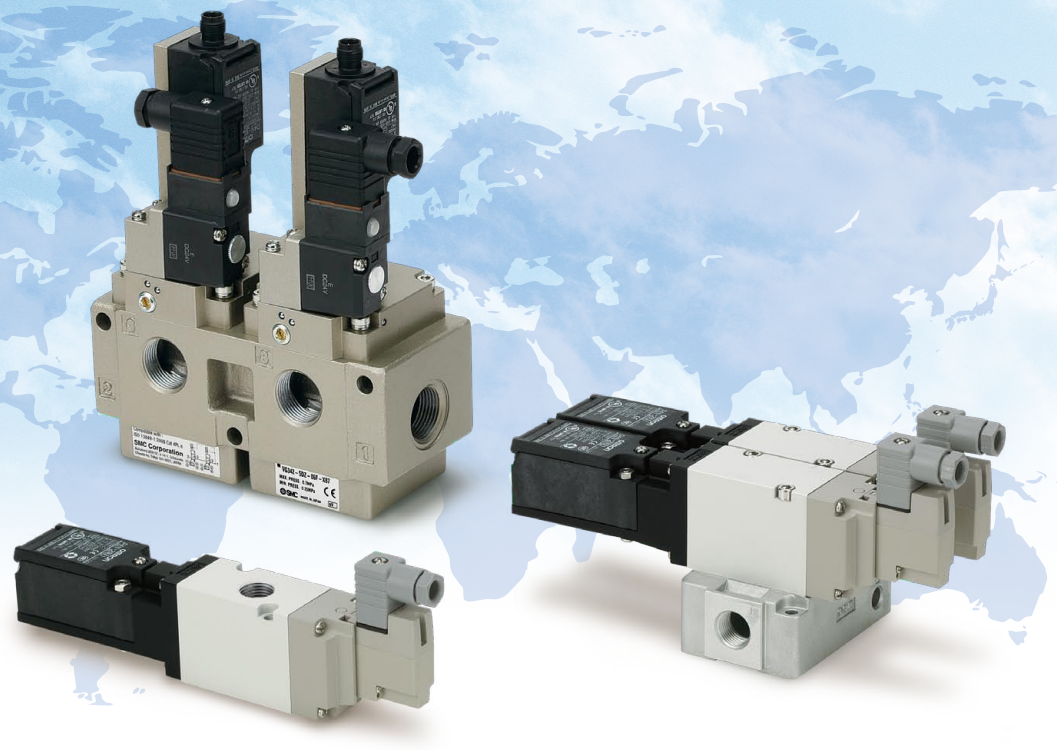
安全規格ISO13849-1の対応

カテゴリ 2~4対応

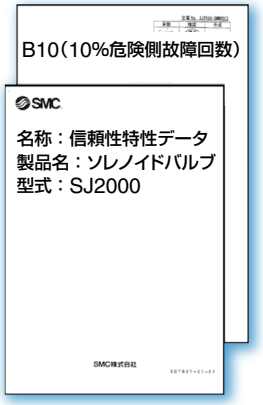
主弁位置検出機能付残圧排気弁により安全制御システム対応



SMCサポート

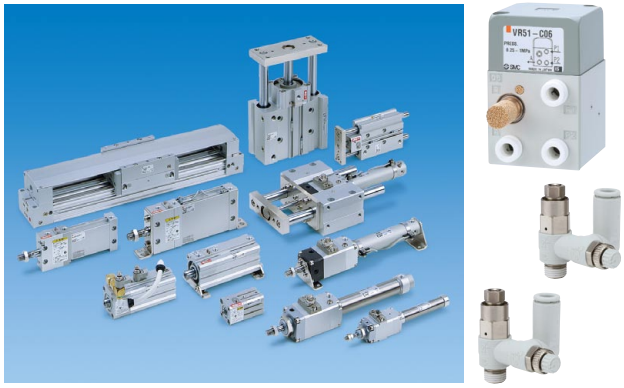
B10(d)/MTTFデータの提出

個々の部品の寿命、故障に関する信頼性特性値を算出し、提出いたします。
(お客さまでMTTFdに変換お願いします。)



機能構成部品の供給

制御システムを構成するための機能部品として製品を提供します。



注) 安全規格の認定を受けた安全部品ではありませんのでご注意ください。

SMC

ISO13849-1の安全規格が2011年12月以降グローバルに展開されました。
各国の規格にも組み込まれています。
例として、欧州の場合の具体的作業の流れを説明します。

（アメリカではANSI、日本ではJIS、中国ではGB等地域毎に組み込まれている規格が違うため、
地域毎に作業の流れが違いますのでご注意ください。）

EN（欧）
ANSI（米）
JIS（日）
GB（中）
・・・・・

機械指令（欧）

ISO12100-1

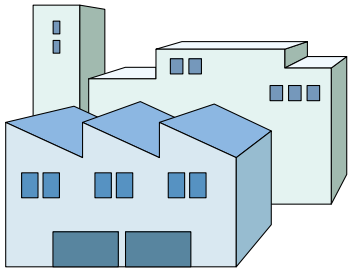
危険箇所の特定や「リスクアセスメント方法」を定義化する規格です。

1. 機械的危険
2. 電気的危険
3. 熱的危険
4. 騒音による危険
5. 振動による危険
6. 放射による危険
7. 材料による危険
8. 非人間工学の危険
9. 使用環境と関連した危険
10. 組み合わせによる危険

ISO13849-1

制御システム安全関連部の設計および妥当性確認の規格です。必要な性能レベルを達成するためにガードスイッチ、インターロック回路等を使って対策します。

- インターロック装置
- 非常停止装置
- ……
- ……



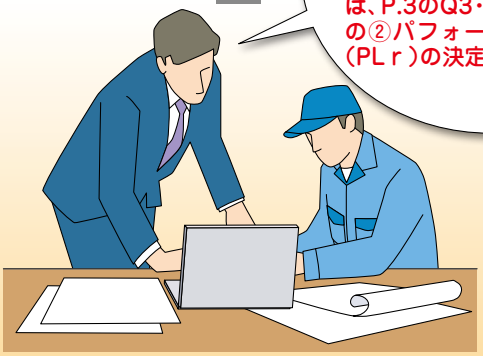
機械指令（欧）→ ISO12100-1
↓
ISO13849-1（安全制御システムのチェック）
↓
（その他の整合規格）
↓
認定

エンドユーザ

作業者の安全を確保するのにレベル"c"以上が必要なのか…。装置メーカに指示しよう。

指示

装置構想



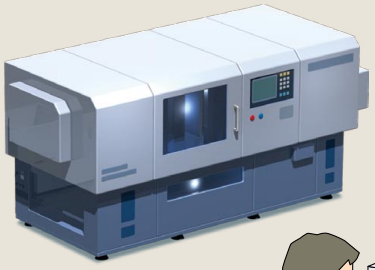
この装置の安全レベルは、a～eの5段階評価で"c"になりますね。
（装置安全のレベルについては、P.3のQ3・Aおよび、P.5の②パフォーマンスレベル（PLr）の決定参照）

第三者機関やコンサルタント等でもチェックできます。
作業者が怪我をするリスクや安全機器と制御回路を確認して危険度のレベルを決めます。

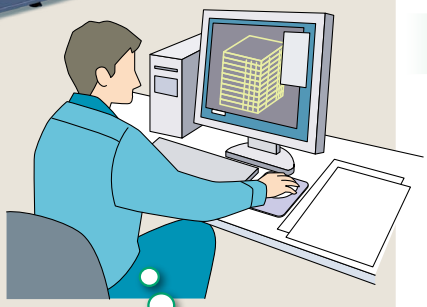
装置構想

装置メーカ

対応



装置設計
装置認証



エンドユーザからの指示でISO13849-1※に適合させないといけない。
空気圧機器の対応はSMCに相談しよう!

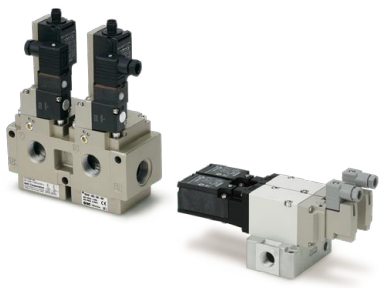
※P.3のQ2および、P.4、5をご参照ください。

ISO13849-1

SMCサポート

主弁位置検出機能付 デュアル残圧排気弁のご提案

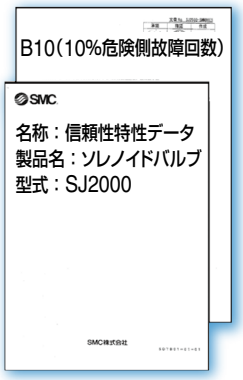
バルブに搭載の位置検出機能が2連の主弁不一致を検出し、直ちにエア遮断機能が作動する安全制御システム対応バルブです。



参照 P.3 P.6 P.12 P.14 P.15

B10(d)/MTTFデータの提出

個々の部品の寿命、故障に関する信頼性特性値を算出し、提出いたします。
(お客さまで、MTTFdに変換お願いします。)



参照 P.13

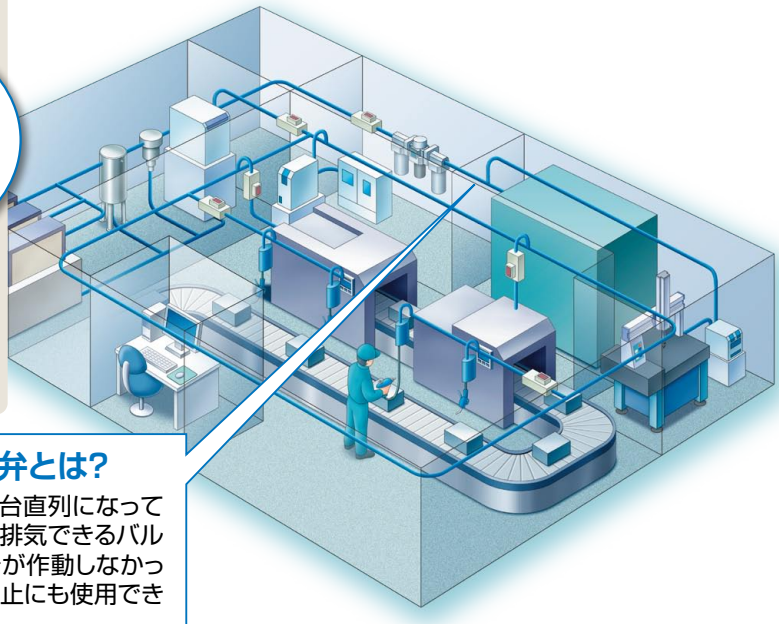
機能構成部品の供給

制御システムを構成するための機能部品として製品を提供します。

参照 P.16 ～ 裏表紙

SMC営業

依頼



主弁位置検出機能付デュアル残圧排気弁とは?

主弁の動きをチェックするスイッチ付3ポート弁が2台直列になっており、1ヶが作動しなくても、もう一方で安全に残圧を排気できるバルブです。例えば、スプール位置スイッチは、バルブ1ヶが作動しなかったことを示し、修復されるまでシステムの再通電の防止にも使用できます。

SMCは安全制御システムに関連する製品の提供ができます。

主弁位置検出機能付デュアル残圧排気弁等関連製品の提供

VG342-□-X87

VP544-□-X538

冗長性がある位置検出バルブ

ISO13849-1 簡単! Q&A

Q1 ISO13849-1の規格でSMC営業がお客様にできることはなんですか?

A 下の3点になります。

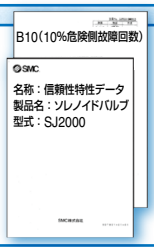
SMCサポート

❶主弁位置検出機能付デュアル残圧排気弁のご提案

1ヶが作動しなくても、もう一方で安全に残圧を排気できるバルブです。例えば、スプール位置スイッチは、バルブ1ヶが作動しなかったことを示し、修復されるまでシステムの再通電の防止にも使用できます。

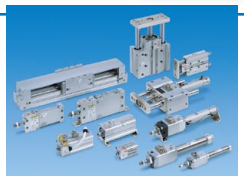
❷B10(d)/MTTFデータの提出

個々の部品の指定された寿命に関する信頼性特性値を算出し、提出いたします。(お客さまで、MTTFdに変換お願いします。)



❸機能構成部品の供給

制御システムを構成するための機能部品として製品を提供します。

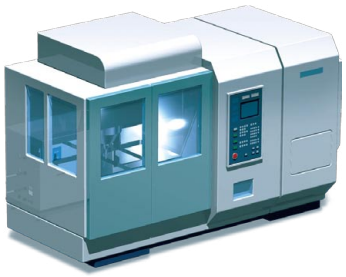


Q2 ISO13849-1の規格を簡単にいうとどんな規格ですか?

A 定義されたリスクのレベルに基づいて、機械制御システム安全関連部の設計と構成が、その機械の危険から人々を保護するのに適切であることを確実にする規格です。

Q3 装置安全のレベル分けは誰がするのですか?

A 装置自体のメカ的な安全装置(システム)や使われている機器の信頼性を評価して、ユーザが行いますが、第三者機関やコンサルタントでもレベル分けができます。そのレベルが、PL(パフォーマンスレベル)と呼ばれています。これがその装置の安全レベルの評価基準となります。



Q4 レベル分けをされたあとどうなりますか?

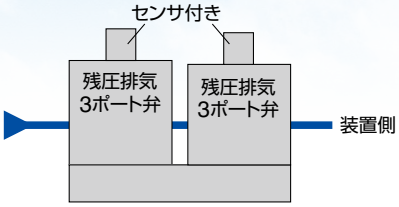
A 要求性能レベルであるPLr決定後、実際の安全制御システムから、PLを求めます。このPLのレベルが、PLrと比較して同等かそれ以上であれば規格適合ですが、満たない場合対策が不充分となります。それでエンドユーザは安全のレベルに従った対策が不充分な場合、安全を確保するための装置導入や、装置改造が必要になります。その指示に従い、例えば、セットメーカは装置の安全を確保するための、部品やシステムを組んで設計することになります。

Q5 客先からISO13849-1の規格を要求された場合、どう対応すべきですか?

A ISO13849-1のパンフレットを持っていきましょう。SMCが提供できるサービス、❶主弁位置検出機能付残圧排気弁の供給、❷データ提出、❸機能構成部品の供給について説明してください。

Q6 主弁位置検出機能付デュアル残圧排気弁って何ですか?

A 安全規格に対応するために、作られた残圧排気弁です。残圧排気3ポート弁が2ヶ直列(アンド回路)に並んでいて、1ヶが故障しても別の1ヶが動いて、残圧排気がされます。これを冗長性機能と呼びます。
また、バルブ動作を確認するセンサが付属されていますのでそのセンサでバルブが正常動作されているかが判かります。また、安全に動作されていない場合は、再通電を防止することができます。



Q7 今後規格が施行されてますが、既設の装置も規格に対応するのですか?

A 2011年12月末に規格が施行され、新規装置は適応が必要になっています。
既設装置については、能力UP等で装置変更など改造が必要になった場合、規格に準拠しなければなりません。そのために機器や回路を安全なものにして規格適合させます。改造でも主弁位置検出機能付残圧排気弁やデータの提供要求、安全機器の必要性が生じます。

Q8 規格で冗長性と言う言葉を聞きますが、冗長性とはなんですか?

A 冗長性とはシステムを構成する要素・部品に予備や安全確保の手段を付加する事で、その一部に故障などがあっても、全体としては停止することなく要求機能を満たす事です。
主弁位置検出機能付残圧排気弁などは、バルブが2つ直列に接続されて一つのバルブが壊れても、もう一つが機能するなど冗長性があると言われます。

Q9 ISO13849-1でカテゴリとよく聞きますが、簡単に言うとどういうことですか?

A ISO13849-1で言われるカテゴリとはPL(実際の安全制御の安全レベル)を決定するための4つの要素の1つであり、安全レベルを安全制御システムの構造(ハードウエア)と信頼性(寿命や故障などの確率論)を組み合わせて5段階に分類します。
カテゴリは、B, 1, 2, 3, 4の5段階があります。

- **カテゴリB, 1**…安全機能が一つのチャネルで遂行できる。単一欠陥で安全機能は損なう。
- **カテゴリ2** ……安全機能が一つのチャネルで遂行できるし、自動チェックができる。
- **カテゴリ3** ……冗長性があるので、単一欠陥で安全機能は損なわない。安全機能を使用の前に毎回チェックする必要がある。未検出の欠陥の累積で安全機能を損なうことがある。
- **カテゴリ4** ……冗長性があるので、単一欠陥で安全機能は損なわない。安全機能を使用の前に毎回チェックする必要がある。未検出の欠陥の累積で安全機能を損なわないこと。(カテゴリ3よりDCおよびMTTFdが高い)

以上のような概要となっています。

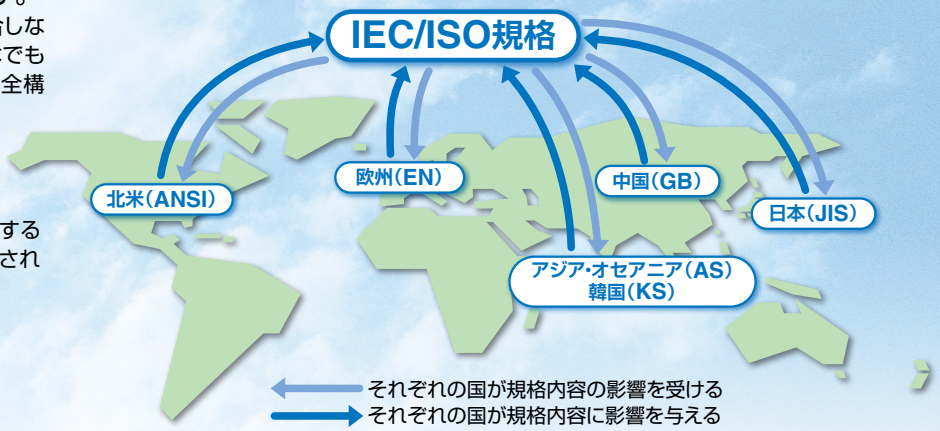
安全規格ISO13849-1にSMCは対応します。

機械安全の概念は、現在国際標準で定められ国際化対応が加速しています。

国際標準の規格(IEC/ISO規格)に適合することが主要な条件になってきています。
(例:欧州では機械指令の整合規格となり、適合しない設備はEU圏内で流通できなくなります。日本でもこの安全概念を取入れ、国際標準に沿う形で安全構築を行う様になってきています。)

国際化対応が加速
WTO/TBT協定の加盟国は、国際規格に準拠する必要があり、各国の規格は、さらに国際的に整合されていきます。

機械安全に関する国際化対応が加速しています。



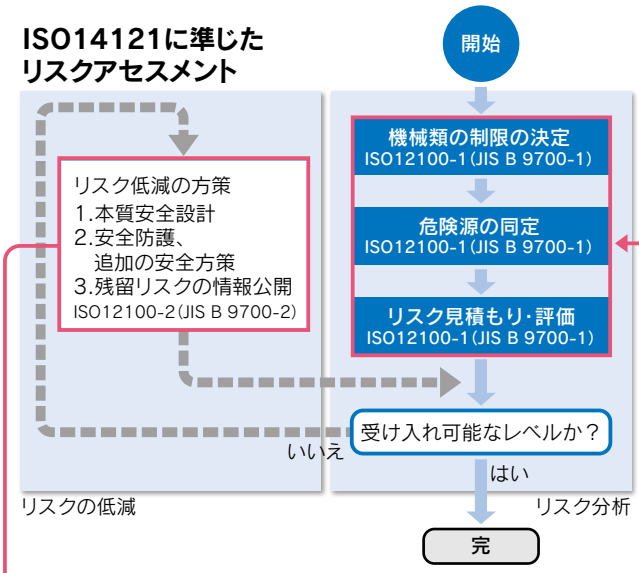
1 リスクアセスメント(危険度の分析)手順

1 リスクの分析とリスク低減

機械またはプロセスの設計責任者は、**必要な安全規格、規制に適合した設計**をする事が求められます。そのためにまず**ISO14121(JIS B 9702)**に準じた方法で、機械全体にある"リスク"を、**ISO12100(JIS B 9702)**の定義を用いて同定し、リスクを見積もり、リスクがあれば低減するために方策を取る事になります。

定義化された機械のリスクは、ISO14121のフローに基づき、機械全体に発生する危険度のチェックと低減を行います。

ISO14121に準じたリスクアセスメント



このリスクの低減が、制御システムに基づく場合、**ISO13849-1で安全制御システム**を評価しリスク低減を図ります。(今まではEN954-1が使用されていました)

リスク見積もり

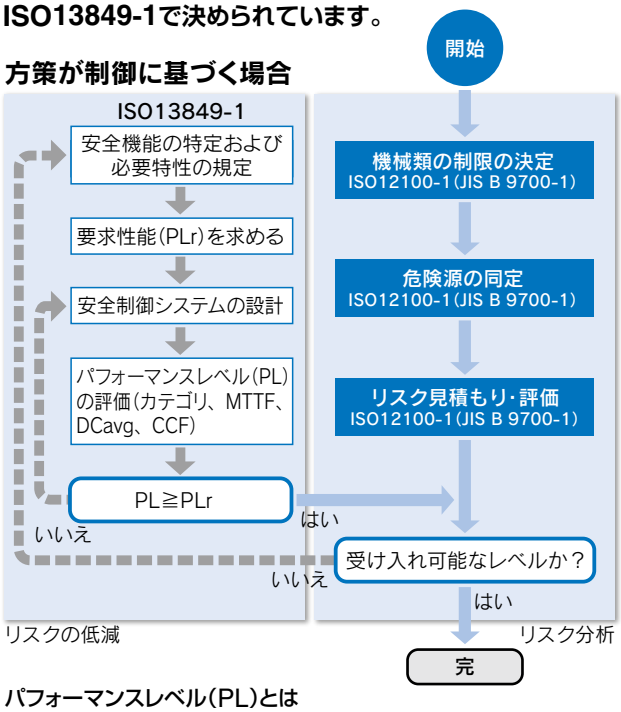
リスクの見積もりの基準となる機械安全の危険源は、ISO12100-1(JIS B 9702)で下記例の様に定義化されています。

①**機械的危険**(押しつぶし、挟まれ、せん断等)
②**電気的危険**(感電、絶縁不良、静電気等)
③**熱的危険**(火災、爆発、やけど等)
④**騒音**による危険
⑤**振動**による危険
⑥**放射**による危険(低周波、電磁波等)
⑦**材料**による危険(有害物質等)
⑧**非人間工学の危険**(ヒューマンエラー等)
⑨**使用環境**と関連した危険
⑩**組合せ**による危険

2 リスク低減の方策が制御に基づく場合

パフォーマンスレベル(PL)で評価され、その評価手順は、ISO13849-1で決められています。

方策が制御に基づく場合



パフォーマンスレベル(PL)とは
機械のリスクのレベルとそれに見合った安全制御システムのレベルを"a"から"e"の5段階で比較評価します。

2 パフォーマンスレベル(PL)の決定

1 評価基準の要求性能レベル(PLr)の決定

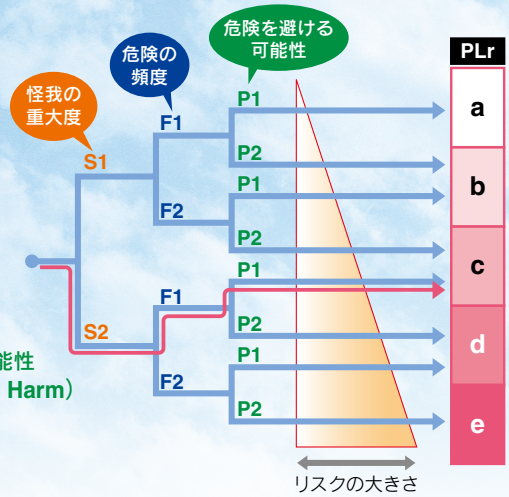
まず、評価基準の要求性能レベル(PLr)を決定します。
要求性能レベル(PLr)は、怪我の重大性(S)、危険にさらされる頻度(F)、危険を避けうる可能性(P)から評価されます。

ISO13849-1:2006

S：怪我の重大度
(Severity of Injury)
S1：軽傷
S2：重傷(後遺症、死亡など)

F：危険にさらされる頻度
(Frequency and/or Exposure to Hazard)
F1：まれに発生するか短時間
F2：頻繁に発生するか長時間

P：危険を避ける、あるいは損害を制限する可能性
(Possibillty of Avoiding Hazard or Limiting Harm)
P1：特定の条件下で可能
P2：不可能



評価例

◎PLrの決定
怪我が重傷(S2)で、危険にまれにさらされ(F1)、危険を避ける事が可能(P1)であれば、PLrは、"c"となります。

◎PLの決定
PL≧PLrより
必要となるPLは"c" "d" "e"となります。

パフォーマンスレベル(PL)を満たすには、4つのパラメータ
❶カテゴリ　❷MTTFd
❸DCavg　❹CCF
の総合した数値が、**要求性能レベル(PLr)**を超えるように設計しなければなりません。

評価例

◎PLを満たすために
装置カテゴリが3の場合
・DCavg=Low
・MTTFd=Medium以上
・CCF=65点以上

または、
・DCavg=Medium
・MTTFd=Low以上
・CCF=65点以上
が、必要となります。

※ PLのパラメータ は下記をご参照ください。

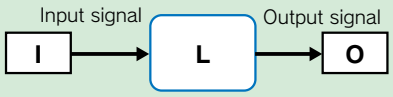
2 実際の安全制御システムのパフォーマンスレベル(PL)の決定

要求性能レベル(PLr)とは別に、実際の**安全制御システムのPLを決定**します。このPLを満たすには、4つのパラメータ❶カテゴリ❷MTTFd❸DCavg❹CCFの総合した数値が、要求性能レベル(PLr)を超える必要があります。

PLのパラメータ			判断基準
❶ ハードウェアの構造	カテゴリ	安全制御システムのアーキテクチャ(I, L, Oの構成) カテゴリは、I(入力機器)，L(論理演算機器)，O(出力機器)で構成されています。	B 1 2 3 4 5通り
❷ 部品の寿命	MTTFd B10d Nop※	①部品単位 1. メーカが用意したMTTF 2. ※Annex C記載のMTTFまたは、B10が与えられている場合は、 $MTTFd=\frac{B10d}{0.1\times Nop}$　$B10d=2\times B10$ ※Nop(その部品が1年間に稼動する回数)、機械の設計者自身が把握しておく必要がある。 ②システム全体 $MTTFd=\frac{1}{\sum_{i=1}^{n}\frac{1}{MTTFdi}}$ $MTTFd=2\times MTTF$	High (30年以上100年未満) Medium (10年以上30年未満) Low (3年以上10年未満) 3通り
❸ システムの信頼性	DCavg DC MTTFd	①部品単位 ※Annex E表1からDCを選ぶ IEC/EN61508, IEC/EC62061やEN954-1などを認証取得した製品を用いれば、計算が容易になります。 ②システム全体 $DCavg=\frac{\sum_{i=1}^{n}\frac{DCi}{MTTFdi}}{\sum_{i=1}^{n}\frac{1}{MTTFdi}}$	High (99%以上) Medium (90%以上99%未満) Low (60%以上90%未満) None (60%未満) 4通り
❹ 設計の確かさ	CCF	※Annex Fのチェックリストのスコアが65点以上あること カテゴリ2以上には、CCFの点数が65点以上求められる。	Yes(65点以上) No(65点未満) 2通り

※ISO13849-1の規格書を参照してください。

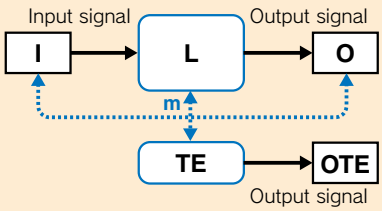
カテゴリB,1,2,3,4の組合せの違いと要約



カテゴリB、カテゴリ1に適用される構造

I：入力機器（例：センサ）
L：論理演算機器
O：出力機器（例：コンタクタ）

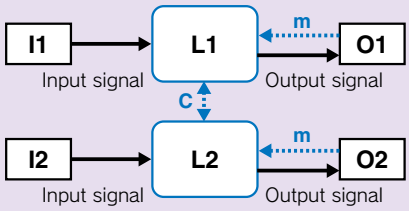
※カテゴリ1のMTTFdはカテゴリBより高いため、安全機能が喪失する可能性はより低いが、故障時には、安全機能の喪失を招くことがある。



カテゴリ2に適用される構造

m ：モニタリング
TE ：点検機器
OTE：点検結果の出力

※カテゴリ2は、故障が起きると、点検と点検の間で安全機能の喪失を招くことがある。



カテゴリ3、カテゴリ4に適用される構造

m：モニタリング
C ：クロスモニタリング

※カテゴリ3は、検出されていない故障の累積により安全機能が働かない場合がある。
※このブロック図に規定されたアーキテクチャの冗長系は物理的な意味だけでなく、単一故障耐性が確認された内部論理も意味する場合がある。

カテゴリ	要件の要約
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。 予想されたストレス（例：振動、EMCなど）に耐えること。
1	カテゴリB＋ 十分に吟味された高信頼性のコンポーネントを使用すること。
2	カテゴリB＋ 安全機能が適切な間隔でチェックされること
3	カテゴリB＋ 単一欠陥で安全機能は損なわないこと。 単一欠陥はできる限り検出されること。
4	カテゴリB＋ 単一欠陥は安全機能実行時、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、欠陥の累積で安全機能を損なわないこと。

標準バルブ

位置検出バルブ

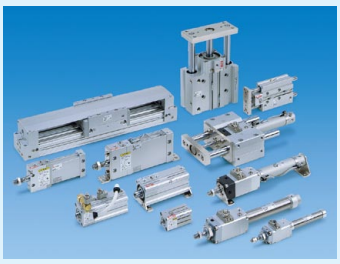
冗長性がある
位置検出バルブ

SMCは安全制御システムに関連する製品の提供ができます。

主弁位置検出機能付
残圧排気弁等
関連製品の提供

安全制御システムは、機械の目的や危険の度合、機械の規模、使用頻度によってその全体の設計が異なります。例えば、「モノを組付ける」を考えた時に、ロボット、ピック&プレース、半自動など目的に応じて様々な違いがあり、装置の構造も異なります。
このような基本的な構造の分類が安全制御システムでいうカテゴリです。

SMCはその他安全に関する推奨製品をラインアップしています。



Simplified procedure for evaluating PL achieved by SRP/CS

❶Category		B	1	2	2	3	3	4
❷MTTFd of each channel								
	Low	a	—	a	b	b	c	—
	Medium	b	—	b	c	c	d	—
	High	—	c	c	d	d	d	e
❸DCavg		None	None	Low	Medium	Low	Medium	High
❹CCF		None		65点以上—				

例：CCFが65以上、カテゴリ3、MTTFd＝Medium、DCavg＝Lowの場合PLは"c"と評価される。

INDEX

安全規格ISO13849-1とSMCの役割 ……P.8
1 安全設計の世界の流れ ……P.8
2 ISO13849-1の安全設計 ……P.8
3 機械類の安全性・制御システムの安全性関連部 ……P.9

リスクアセスメント(危険度の分析)手順 ……P.9
1 リスク低減の方策が制御に基づく場合 ……P.10
◎評価基準の要求性能レベル(PLr)の決定……P.10
◎実際の制御システムレベル(PLr)の決定 ……P.11
2 4つのパラメータでPLの決定 ……P.12

PLを決定する4つのパラメータ ……P.12
1 カテゴリについて ……P.12
2 MTTFdについて ……P.13
3 DCavgについて……P.13
4 CCFについて ……P.13

SMCの対応 ……P.13

提案バルブ、配線例(カテゴリB～4) ……P.14

空圧機器推奨製品 ……P.16

空圧機器汎用製品 ……P.18

1 方向制御機器 …… P.16

2 アクチュエータ …… P.17

3 駆動制御機器 …… P.18

4 検出スイッチ …… 裏表紙

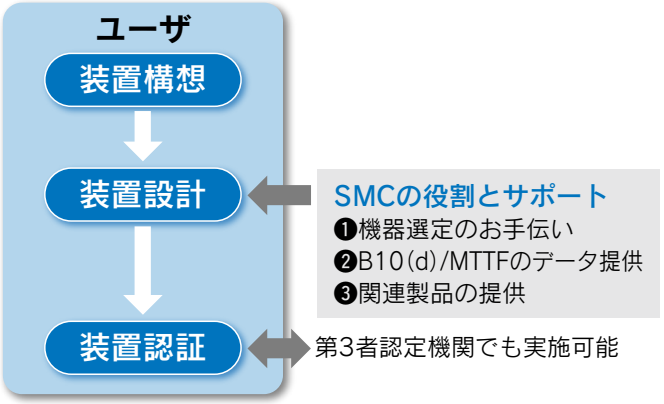
安全規格ISO13849-1とSMCの役割

ISO13849-1：2006（Safety-related part of control system）は、設備や機械の制御システムに、定量的で明確なアセスメント（評価･査定）方法を提供する目的で制定されました。
このISO13849-1は、欧州で新機械指令（2006/42/EC、2009年12月29日より施行）の整合規格として必須となります。

そして、これから装置や機械の安全設計を検討される設備メーカやエンドユーザの方々にSMCは、

❶機器選定のお手伝い
❷B10（d）注1）/MTTFのデータ等信頼性データのご提供
❸安全関連製品のご提供

を行っていきます。



注1）**B10（d）（摩耗故障を持たない電子機器の場合のみMTTF）データ**
当社から提供される信頼性特性値（B10（d）またはMTTF）は、設備に使用される部品固有の値です。
安全カテゴリを査定する際のパラメータへの変換は、お客様で行っていただく必要があります。
尚、この値は標準状態（当社社内試験条件）におけるものであり、お客様の設備稼働条件で保証されるものではありません。

1 安全設計の世界の流れ

現在日本での機械設計の基準となるJIS規格は、国際的な標準規格であるISO規格（国際標準化機構）やIEC規格（国際電気会議）を取り入れるようになり、多岐に渡り整合化が進んでいます。

この背景として、機械安全の概念が、国際標準で定められ国際化対応が加速している事から来ています。

そして国際標準の規格（IEC/ISO規格）に適合することが機械安全を満たす主要な条件になってきています。

例えば、欧州では、圏内で強制力のあるEU指令の一つである新機械指令（2006/42/EC）が2009年12月29日より法令化されています（法令化されたが、旧規格EN954の適応も2年延長となった。結果実際の施行は2011年12月29日からとなる）。この新機械指令に対応するためには、このISO13849-1が整合規格として必須とされています。
ISO13849-1自体は義務で強制力がない規格ですが、この機械指令適合のため、日本でも特に欧州向けに設備の出荷を検討している設備メーカやエンドユーザの方々から当社を含め空圧メーカに対応の依頼が来ています。

こういった背景の中で、世界的レベルで機械またはプロセスの設計責任者は、必要な安全規格、規制に適合した設計をする事が求められます。

この国際的な規格の中で、空圧・油圧・特定の電気機械が使用される装置や機械の安全制御システムに要求される原則や性能を規定した規格がISO13849-1です。

2 ISO13849-1の安全設計

ISO13849-1：2006以前に使われてきた安全制御システムのアーキテクチャ（安全構造）は、設備や機械の内部構成を中心とした確定論的なもので、例えば、内部部品の経年変化による安全機能の喪失等は考慮されていませんでした。このため機械安全の考え方を、機能および信頼性の面から規定しようとする流れに変わってきました。このため、今回改訂されたISO13849-1：2006では、確定論的な機能と確率論的な信頼性を融合させています。これは、従来の構造による定義に加え、部品レベルの危険側故障までの寿命や、危険側故障を検出するなどの安全制御システムを確率論的に評価する二層構造の定義になりました。
この定義により実際の機械の使用状況に合せて機械安全を定量的に評価できるようになりました。

3 機械類の安全性・制御システムの安全性関連部

ISO13849-1には、機械設計のための一般原則が定められています。制御システムの安全関連部(SRP/CS)の設計および統合の原則に関する安全要求事項について規定し、安全機能を実施するための必要な性能レベルを含む特性を規定しています。
そして使用する技術およびエネルギーの種類(電気、油圧、空気圧、機械的など)は問わず、全ての種類の機械類に適用されます。
ISO13849-2には妥当性確認についても定められており、設計者が示した設計上の理論的根拠を用い、ISO13849-1に従って、制御システムの安全関連部について、安全機能および達成されるカテゴリの解析および試験による妥当性確認時の従うべき手順および条件を規定しています。

リスクアセスメント(危険度の分析)手順

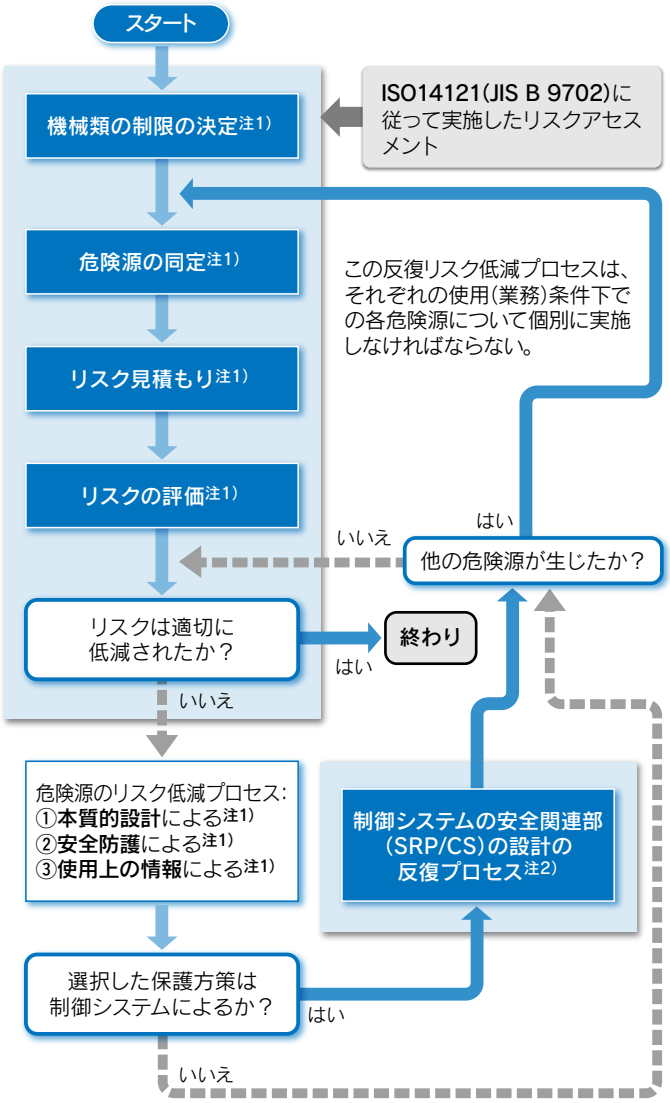
具体的安全設計の手法をご説明します。

まずISO14121に準じた方法で、機械全体にある"機械のリスク"を、ISO12100(JIS B 9702)の定義を用いて同定し、リスクを見積もり、リスクがあれば低減するために方策を取る事になります。これをリスクアセスメントと呼びます。

リスクの見積もりの基準となる機械安全の危険源は、ISO12100-1(JIS B9 702)で下記例の様に定義化されています。
①機械的危険(押しつぶし、挟まれ、せん断等)
②電気的危険(感電、絶縁不良、静電気等)
③熱的危険(火災、爆発、やけど等)
④騒音による危険
⑤振動による危険
⑥放射による危険(低周波、電磁波等)
⑦材料による危険(有害物質等)
⑧非人間工学の危険(ヒューマンエラー等)
⑨使用環境と関連した危険
⑩組合せによる危険

この基準を用いて、次の作業フローに則りリスクの決定、同定、見積もりを行い、問題がある場合は、リスク低減のための方策を検討する事になります。

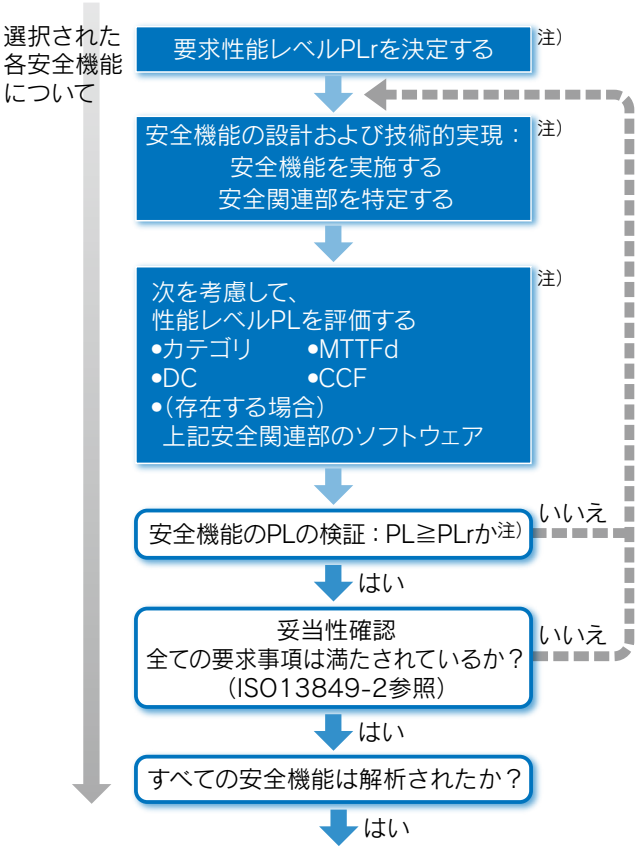
リスクアセスメント/リスク低減の概要



注1) ISO12100-1(JIS B 9700-1)を参照。
注2) ISO13849-1およびP.10■を参照。

1 リスク低減の方策が制御に基づく場合

このリスクの低減が、制御システムに基づく場合、ISO13849-1で安全制御システムの機械安全を評価しリスク低減を図ります。（今までは機械部品のEN954-1と電子部品IEC61508が適用されていた部分です）



注）ISO13849-1を参照。

ISO13849-1の安全制御システムのリスクをどう評価し低減するかの基準がパフォーマンスレベル（PL）です。
パフォーマンスレベルとは、部品レベルの時間的な要素など、信頼性を確率論的に評価する定義を定量的に表すための、共通の評価尺度で、機械のリスクのレベルとそれに見合った安全制御システムのレベルを"a"から"e"の5段階で比較評価します。

パフォーマンスレベル（PL）を満たすには、4つのパラメータ①カテゴリ②MTTFd③DCavg④CCFの総合した数値が、要求性能レベル（PLr）を超えるように設計しなければなりません。

◎評価基準の要求性能レベル（PLr）の決定

手法として、まず評価の基準の要求性能レベル（PLr）を決定します。
要求性能レベル（PLr）は、怪我の重大性（S）、危険にさらされる頻度（F）、危険を避けうる可能性（P）から評価されます。

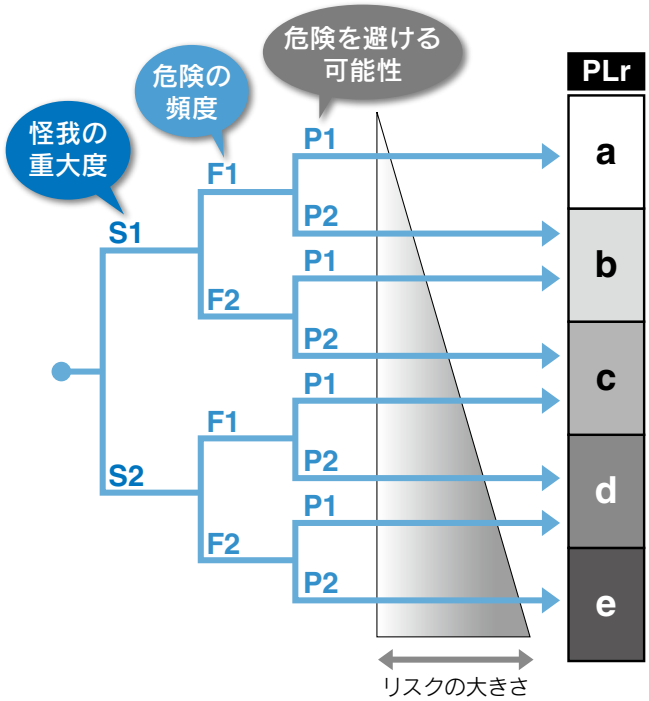
評価例）怪我が重傷（S2）で、危険にまれにさらされ（F1）、危険を避ける事が可能（P1）であれば、PLrは、"c"となります。

ISO13849-1：2006

S：怪我の重大度
（Severity of Injury）
S1：軽傷
S2：重傷（後遺症、死亡など）

F：危険にさらされる頻度
（Frequency and/or Exposure to Hazard）
F1：まれに発生するか短時間
F2：頻繁に発生するか長時間

P：危険を避ける、あるいは損害を制限する可能性
（Possibillty of Avoiding Hazard or Limiting Harm）
P1：特定の条件下で可能
P2：不可能



◎実際の制御システムレベル(PLr)の決定

次に4つのパラメータで実際の安全制御システムのパフォーマンスレベル(PL)の決定を行います。
要求性能レベルPLrとは別に、実際の安全制御システムレベルのPLを決定します。
PLは、4つのパラメータ(①カテゴリ②MTTFd③DCavg ④CCF)の組合せで総合的に決定できます。

①**カテゴリ**：安全制御システムの構造
②**MTTFd(B10d)**：各チャンネルの危険側故障などでの平均時間
③**DCavg**：システム全体の故障検出の信頼性
④**CCF**：予見できる共通の原因に対するシステム全体の信頼性

PLのパラメータ			判断基準
① ハードウェアの構造	カテゴリ	安全制御システムのアーキテクチャ(I, L, Oの構成) カテゴリは、I(入力機器), L(論理演算機器), O(出力機器)で構成されています。	B 1 2 3 4 5通り
② 部品の寿命	MTTFd B10d Nop※	①部品単位 1. メーカが用意したMTTF 2. ※Annex C記載のMTTFまたは、B10が与えられている場合は、 $MTTFd=\frac{B10d}{0.1\times Nop}$　$B10d=2\times B10$ ※Nop(その部品が1年間に稼動する回数)、機械の設計者自身が把握しておく必要がある。 ②システム全体 $MTTFd=\frac{1}{\sum_{i=1}^{n}\frac{1}{MTTFdi}}$ $MTTFd=2\times MTTF$	High (30年以上100年未満) Medium (10年以上30年未満) Low (3年以上10年未満) 3通り
③ システムの信頼性	DCavg DC MTTFd	①部品単位 ※Annex E表1からDCを選ぶ IEC/EN61508, IEC/EC62061やEN954-1などを認証取得した製品を用いれば、計算が容易になります。 ②システム全体 $DCavg=\frac{\sum_{i=1}^{n}\frac{DCi}{MTTFdi}}{\sum_{i=1}^{n}\frac{1}{MTTFdi}}$	High (99%以上) Medium (90%以上99%未満) Low (60%以上90%未満) None (60%未満) 4通り
④ 設計の確かさ	CCF	※Annex Fのチェックリストのスコアが65点以上あること カテゴリ2以上には、CCFの点数が65点以上求められる。	Yes(65点以上) No(65点未満) 2通り

※ISO13849-1の規格書を参照してください。

この信頼性のパラメータであるMTTFdとDCavgは数式により、CCFはチェックリスト方式で求められます。
それぞれのパラメータは、基準値を使って、MTTFdは3通り、DCavgは3通り、CCFは2通りに分類されます。
PLはこれら4つのパラメータにより総合的に評価され、該当するPLが求められます。

結果これら4つの要素①**カテゴリ**②**MTTFd**③**DCavg**④**CCF**を組合せた総合評価でPLが決定されます。

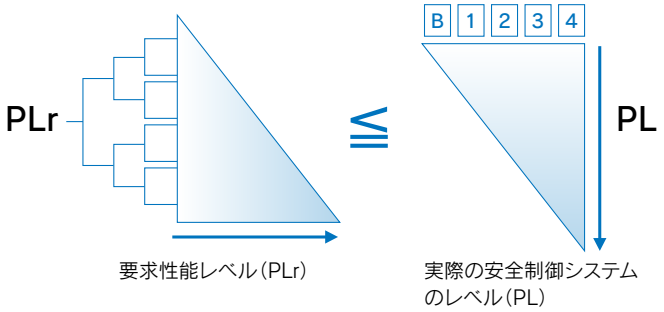
Simplified procedure for evaluating PL achieved by SRP/CS

Category	B	1	2	2	3	3	4
MTTFd of each channel							
Low	a	—	a	b	b	c	—
Medium	b	—	b	c	c	d	—
High	—	c	c	d	d	d	e
DCavg	None	None	Low	Medium	Low	Medium	High
CCF	None		65点以上—				

例：CCFが65以上、カテゴリ3、MTTFd＝Medium、DCavg＝Lowの場合PLは"c"と評価される

2 4つのパラメータでPLの決定

安全制御システムの性能レベル(PL)は、常に要求性能レベル(PLr)と同等かそれ以上である事が求められます。



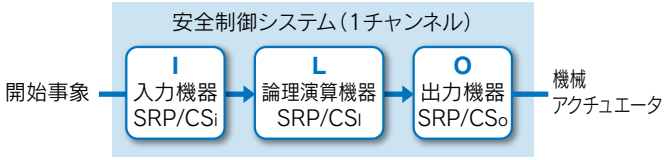
a, b, c, d, eで表した4つのパラメータ①カテゴリ②MTTFd③DCavg④CCFの総合した結果であるPLが、PLrを超えればISO13849-1を満たしているという事になります。

PLを決定する4つのパラメータ

1 カテゴリについて

制御システムの安全関連部(ハードウェア)の構造についてのパラメータです。安全を確保するための構造は、機械の目的や危険の度合い、機械の規模、使われる頻度によって構造が変わります。この構造の基本的分類がカテゴリです。
カテゴリの基本構造は、I(入力機器), L(論理演算機器), O(出力機器)で図式化されます。

ISO13849-1で考える安全機能は、I(入力機器), L(論理演算機器), O(出力機器)を直列に接続した1チャンネルとみなします。



開始事象：押しボタンの手動操作、ドアの開口

(安全制御システム)

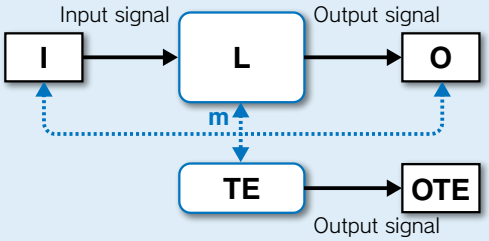
I (入力機器)：開始事象の検出機器(センサ)
L (論理演算機器)：リレーシーケンス回路
PLC制御プログラム
O (出力機器)：電磁開閉器、出力リレー、電磁切換弁

機械アクチュエータ：モータ、流体(油、空気)アクチュエータ
※流体アクチュエータは適用されない。

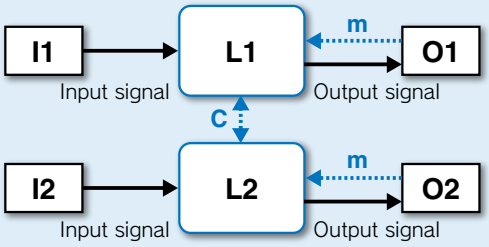
Iは開始事象の検出機器の圧力センサ、Lはリレーシーケンス回路、PLC制御プログラム、Oは電磁開閉器、出力リレー、電磁切換弁となる。

カテゴリには、下記の様にB～4までの5段階があり、安全制御システムのI(入力機器)、L(論理演算機器)、O(出力機器)の、構造が異なります。段階が上がるに伴い、各安全関連部に対する要求も高くなります。

カテゴリB、カテゴリ1に適用される構造
I：入力機器(例：センサ)
L：論理演算機器
O：出力機器(例：コンタクタ)
※カテゴリ1のMTTFdはカテゴリBより高いため、安全機能が喪失する可能性は低いが、故障時には、安全機能の喪失を招くことがある。



カテゴリ2に適用される構造
m ：モニタリング
TE ：点検機器
OTE：点検結果の出力
※カテゴリ2は、故障が起きると、点検と点検の間で安全機能の喪失を招くことがある。



カテゴリ3、カテゴリ4に適用される構造
m：モニタリング
C ：クロスモニタリング
※カテゴリ3は、検出されていない故障の累積により安全機能が働かない場合がある。
※このブロック図に規定されたアーキテクチャの冗長系は物理的な意味だけでなく、単一故障耐性が確認された内部論理も意味する場合がある。

2 MTTFdについて

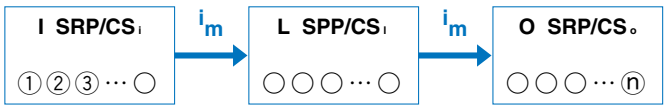
MTTFdは、安全制御システムにおいて、安全機能を喪失するまでの平均的な時間を示します。

機械設備の生産者は、PLを評価するために、安全制御システムに使用されている個々の部品の信頼性データ(MTTF, B10)を必要としています。
安全機能の喪失は、システムを構成する部品の故障が引き金になるので、個々の部品の平均故障寿命がそのベースになるためです。

MTTFdの基準は下記の様になります。

MTTFd	
低	3年≦MTTFd＜10年
中	10年≦MTTFd＜30年
高	30年≦MTTFd＜100年

安全制御システムのI, L, Oの1チャンネルが、n個の部品で構成されている場合のMTTFdは以下のようになります。信頼性工学では、1つのシステムが故障する確率は、そのチャンネルを構成する一つ一つの構成部品の故障率の総和で表されます。危険側故障についても同じです。危険側故障率と危険側平均故障時間の間には逆数の関係が成り立ちます。したがってシステム全体の危険側平均故障時間(MTTFd)は、個々の部品の危険側故障時間(MTTFdi)の逆数の総和で求められる事になります。



$$MTTFd = \frac{1}{\sum_{i=1}^{n} \frac{1}{MTTFdi}}$$

MTTFd：個々の部品の平均故障寿命

当社から提供するB10(d)(摩耗故障を持たない電子機器の場合のみMTTF)データについて補足いたします。
弊社から提供される信頼性特性値(B10(d)またはMTTF)は、設備に使用される部品固有の値です。
安全カテゴリを査定する際のパラメータへの変換は、ユーザ側で行っていただく必要があります。なお、この値は標準状態(当社社内試験条件)におけるものであり、お客様の設備稼働条件で保証されるものではありませんのでご注意ください。

3 DCavgについて

安全制御システム全体の信頼性の指標である平均自己診断率をDCavg(average Diagnostic Coverage)で定めています。
部品のみならずソフトウェアを含めたシステム全体の機能の信頼性を評価します。

DC	
なし	DC＜60%
低	60%＜DC＜90%
中	90%＜DC＜99%
高	99%≦DC

4 CCFについて

共通原因故障をCCF(Common Cause Failure)で定め、安全制御システム全体の機能がある共通の原因によって損なわれないようになっているか設計的なロバスト性の指標となります。
制御システムの安全関連部のあらゆる部分を考慮しなければならず、方策が部分的にだけに果たされると、得点は無くなり、この得点が65点以上で合格となります。

SMCの対応

この設備や機械向けの安全規格であるISO13849-1について、SMCは設備メーカやユーザの方々に、下記3点のサポートをさせていただきます。

①機器選定のお手伝い
SMCの空圧機器が関連する箇所の規格概略のご説明と、設備メーカやユーザの方々が構想された機器構成に使用できる適正機器の選定をいたします。

②B10(d)/MTTFのデータのご提供
設備メーカやユーザの方々でPL(パフォーマンスレベル)を評価される際に必要となるパラメータの一つであるMTTF/B10(d)のデータをご提供します。

③安全回路関連製品のご提供
SMCは、この安全規格のカテゴリに対応した製品を供給いたします。

提案バルブ、配線例

エアをエネルギー源として使用する装置におけるエアの供給／遮断をする制御回路について、カテゴリ毎の推奨バルブとその使用例を以下に示します。ただし、これらの使用例は参考回路であり、安全システムの一部の構成部分ですので、実際の回路につきましては、他関連規格に準拠していただくとともに、システム全体の安全性につきましては、第三者認定機関の確認を得る事を推奨します。

カテゴリB, 1

カテゴリの要求事項の要約

カテゴリ	要求事項の要約	システム挙動	安全達成のための使用原理	各チャンネルのMTTFd	DCavg（自己診断率）	CCF（共通原因故障）
B	基本的安全原理の使用	障害発生が、安全機能の喪失（発生確率は1＜B）	構成部品の選択	低～中	なし	関連しない
1	Bの要求事項＋十分に吟味された（構成部品＋安全原理）			高		

カテゴリの要求事項の組合せ

Category	B	1	2	2	3	3	4
MTTFd of each channel							
Low	a	—	a	b	b	c	—
Medium	b	—	b	c	c	d	—
High	—	c	c	d	d	d	e
DCavg	None	None	Low	Medium	Low	Medium	High

カテゴリの要求事項の指定構造

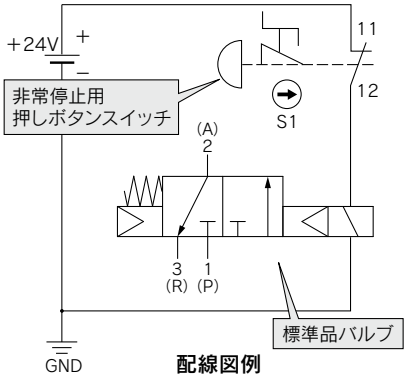
カテゴリB、カテゴリ1に適用される指定構造

- **I：入力機器**（例：センサ）
- **L：論理演算機器**
- **O：出力機器**（例：コンタクタ）

提案バルブ

システム設計者が汎用部品を選択

電気機器：
カテゴリ1に対応できる市販の電気機器



配線図例

カテゴリ2

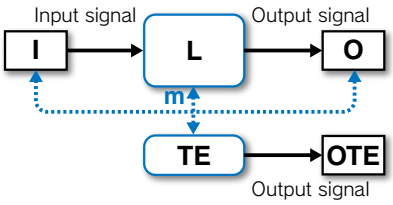
カテゴリの要求事項の要約

カテゴリ	要求事項の要約	システム挙動	安全達成のための使用原理	各チャンネルのMTTFd	DCavg（自己診断率）	CCF（共通原因故障）
2	・Bの要求事項＋十分に吟味された安全原理 ・安全機能は、適切な間隔でチェック	チェックとチェック間で安全機能の喪失	構造による	低～高	低～中	65点以上

カテゴリの要求事項の組合せ

Category	B	1	2	2	3	3	4
MTTFd of each channel							
Low	a	—	a	b	b	c	—
Medium	b	—	b	c	c	d	—
High	—	c	c	d	d	d	e
DCavg	None	None	Low	Medium	Low	Medium	High

カテゴリの要求事項の指定構造



カテゴリ2に適用される指定構造

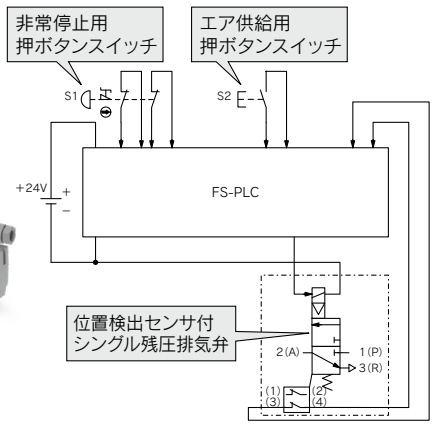
- **m ：モニタリング**
- **TE ：点検機器**
- **OTE：点検結果の出力**

提案バルブ

位置検出センサ付
シングル残圧排気弁
（VP542-□-X536
VP742-□-X536）

電気機器：
カテゴリ2に対応できる市販の電気機器

安全PLCを用いた配線図例（カテゴリ2）



カテゴリ3, 4

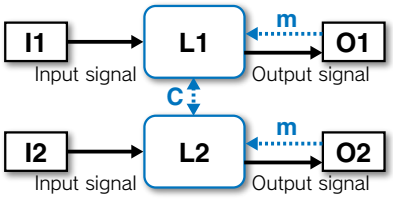
カテゴリの要求事項の要約

カテゴリ	要求事項の要約	システム挙動	安全達成のための使用原理	各チャンネルのMTTFd	DCavg（自己診断率）	CCF（共通原因故障）
3	・Bの要求事項＋十分に吟味された安全原理 ・単一の障害では、安全機能の喪失はない ・単一の障害は検出できる	・単一の障害時、安全機能の実施 ・すべての障害は検出しない ・検出できない障害の蓄積で安全機能の喪失	構造による	低～高	低～中	65点以上
4	・Bの要求事項＋十分に吟味された安全原理 ・単一の障害では、安全機能の喪失はない かつ、 ・単一の障害は次の動作要求時、または、それ以前に検出できる。それがない場合、障害の蓄積が安全機能を喪失しない	・障害発生時、安全機能の実施 ・蓄積障害の検出は安全機能の確率をUP（高DC） ・障害は安全機能の喪失を防ぐことができるうちに検出		高	高	

カテゴリの要求事項の組合せ

Category	B	1	2	2	3	3	4
MTTFd of each channel							
Low	a	—	a	b	b	c	—
Medium	b	—	b	c	c	d	—
High	—	c	c	d	d	d	e
DCavg	None	None	Low	Medium	Low	Medium	High

カテゴリの要求事項の指定構造



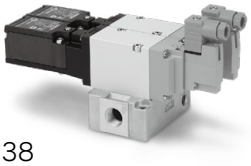
カテゴリ3、カテゴリ4に適用される指定構造

m：モニタリング
C：クロスモニタリング

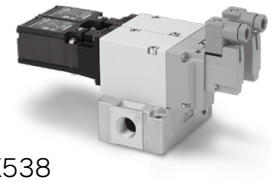
※このブロック図に規定されたアーキテクチャの冗長系は物理的な意味だけでなく、単一故障耐性が確認された内部論理も意味する場合がある。

提案バルブ

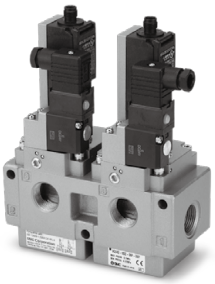
●位置検出センサ付デュアル残圧排気弁



VP544-□-X538

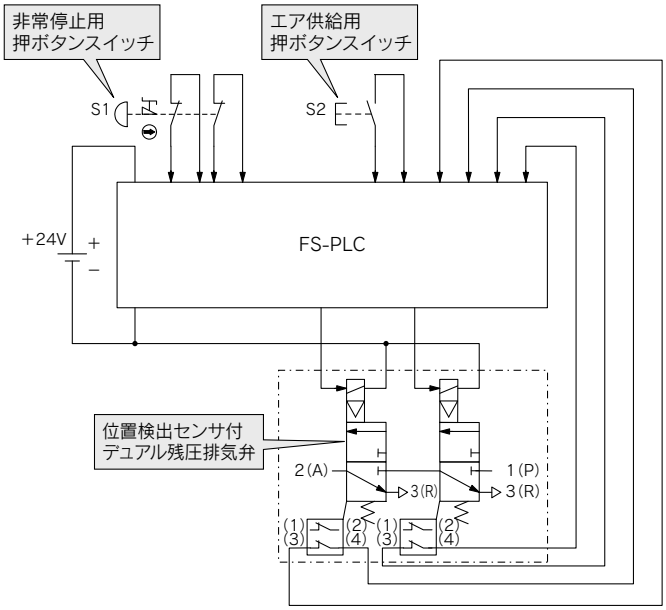


VP744-□-X538



VG342-□-X87

安全PLCを用いた配線図例（カテゴリ3,4）



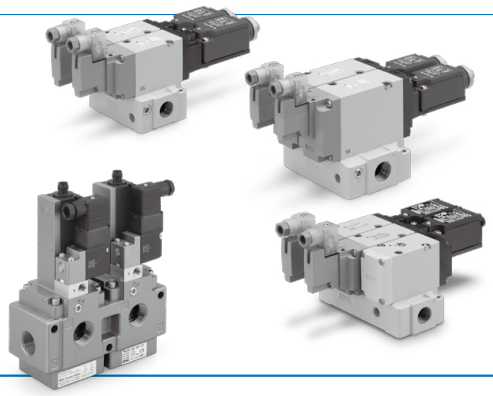
空圧機器推奨製品

装置自体の安全化をサポートするために下記製品を使用することができます。ただしこれらの製品は、機械の制御システムを構成するための機能部品であり、安全規格ISO13849-1の認証は取れておりません(VG342-□-X87, VP542-□-X536, VP544-□-X538, VP742-□-X536, VP744-□-X538以外)。実際の制御システム全体の安全性につきましては、第三者認定機関の確認を得る事を推奨します。

1 方向制御機器

位置検出センサ付デュアル残圧排気弁

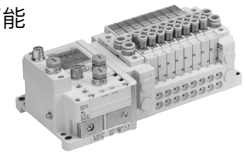
・位置検出が可能
・冗長性がある位置検出が可能

カテゴリ	型式		特長・仕様
カテゴリ**2**	残圧排気弁 VP542-□-X536 VP742-□-X536		・バルブ主弁の位置検出ができる
カテゴリ**3,4**	デュアル残圧排気弁 VP544-□-X538 VP744-□-X538 ソフトスタートアップ機能付 デュアル残圧排気弁 VP544-□-X555 デュアル残圧排気弁 VG342-□-X87		・バルブ主弁の位置検出ができる ・バルブが2連あり、どちらかが不一致で動かない場合、残りのバルブで残圧を排出する。

詳細については、P.G Informationをご参照ください。

残圧排気弁付仕様

・長時間の中間停止、位置保持が可能
・各バルブ毎にエア供給停止可能

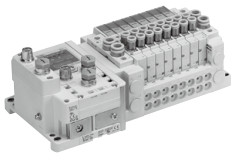


対象機種

名称	シリーズ
5ポートソレノイドバルブ	**SY3000/5000**

背圧防止弁仕様

・背圧によるアクチュエータの誤動作防止

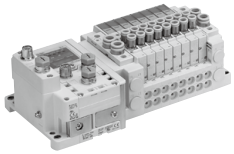


対象機種

名称	シリーズ 直接配管
4ポートソレノイドバルブ	**SJ**
5ポートソレノイドバルブ	**SY3000/5000**
5ポートソレノイドバルブ	**S0700**
5ポートソレノイドバルブ	**VQ**
5ポートソレノイドバルブ	**VQC**
5ポートソレノイドバルブ	**VQZ**
5ポートソレノイドバルブ	**SQ**
5ポートソレノイドバルブ	**VQ7**

スイッチ付仕様

・各バルブの信号を個別に遮断

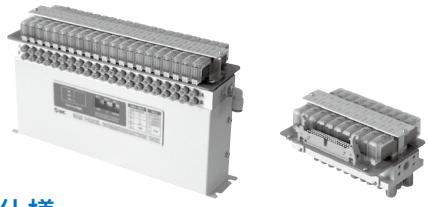


対象機種

名称	シリーズ
5ポートソレノイドバルブ	**SY3000/5000**

インターロック付仕様

・個別コモン配線可能

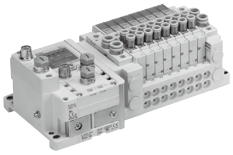


対象機種

名称	シリーズ
5ポートソレノイドバルブ	**SV**
5ポートソレノイドバルブ	**VQC**

分離電源仕様

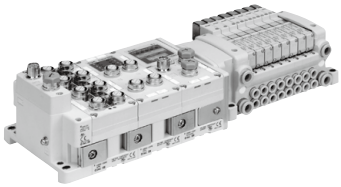
・電源毎に各バルブの信号を個別に遮断



対象機種

シリーズ	適用バルブ
EX250	SY3000/5000 VQC1000, 2000, 4000, S0700

断線短絡検出機能付



対象機種

シリーズ	適用バルブ
EX600	SY3000/5000 VQC1000, 2000, 4000, S0700

両手操作仕様

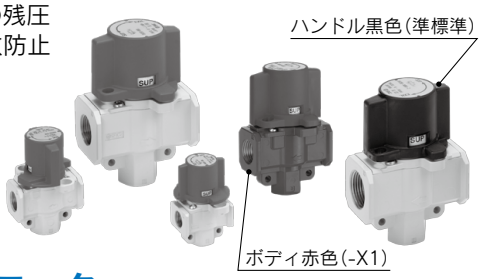
・回路の安全対策機器
・両手同時操作時に出力信号による
　回路の安全対策

対象機種

名称	シリーズ
両手操作用コントローラバルブ	**VR51**

残圧抜き仕様

・空気圧ラインの残圧
　排気による事故防止



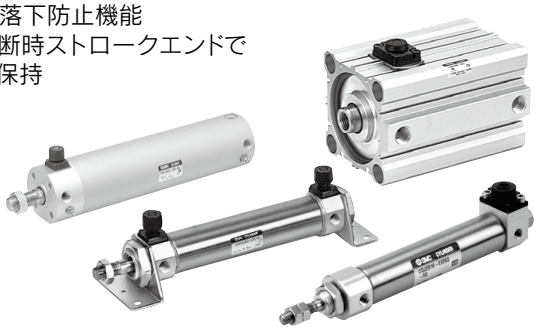
対象機種

名称	シリーズ
残圧抜き3ポート弁 (OSHA規格対応　鍵穴付残圧抜き3ポート弁)	**VHS**

2 アクチュエータ

エンドロック仕様

・確実な落下防止機能
・エア遮断時ストロークエンドで
　ワーク保持



基本形エアシリンダ

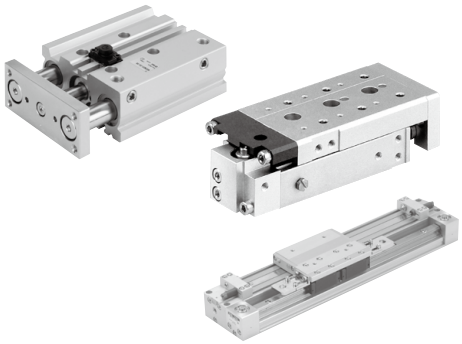
形状	型式	チューブ内径
丸形	**CBJ2**	ø16
	CBM2	ø20～ø40
	CBG1	ø20～ø100
	CBA2	ø40～ø100
	MBB	ø32～ø100
角形	**CBQ2**	ø20～ø100

空圧機器汎用製品

装置自体の安全化をサポートするために下記製品を使用することができます。ただしこれらの製品は、機械の制御システムを構成するための機能部品であり、安全規格ISO13849-1の認証は取れておりません(VG342-□-X87, VP542-□-X536, VP544-□-X538, VP742-□-X536, VP744-□-X538以外)。実際の制御システム全体の安全性につきましては、第三者認定機関の確認を得る事を推奨します。

エンドロック仕様

・確実な落下防止機能
・エア遮断時ストロークエンドでワーク保持



ガイド付シリンダ

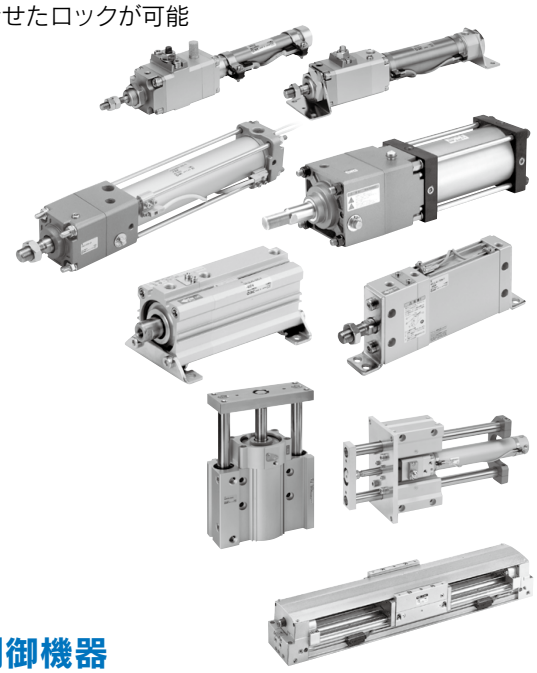
形状	型式	チューブ内径
シャフトガイド形	MGG	ø20～ø100
	MGP	ø20～ø100
	CXS	ø6～ø32
	CXW	ø10～ø32
	MGZ	ø40～ø63
	MTS	ø12～ø40
リニアガイド形	MXS	ø8～ø25
	MXQ	ø8～ø25

メカジョイント式ロッドレスシリンダ

形状	型式	チューブ内径
リニアガイド形	MY1H	ø16～ø40

ロック付仕様

・非常停止による落下防止機能
・ワークに合せたロックが可能



基本形エアシリンダ

形状	型式	チューブ内径
丸形	CLJ2	ø16
	CLM2	ø20～ø40
	CNG	ø20～ø40
	CNA2	ø40～ø100
	MNB	ø32～ø100
	CNS	ø125～ø160
	CLS	ø125～ø250
	CL1	ø40～ø160
	C95N	ø32～ø100
角形	CLQ	ø20～ø100
	RLQ	ø32～ø63
短形	MLU	ø25～ø50

ガイド付シリンダ

形状	型式	チューブ内径
シャフトガイド形	MLGP	ø20～ø63
	MLGC	ø20～ø40
	CLK1	ø32～ø63

ブレーキ付メカジョイント式ハイロッドレスシリンダ

形状	型式	チューブ内径
カムフォロアガイド形	ML1C	ø25～ø40

3 駆動制御機器

残圧排気仕様

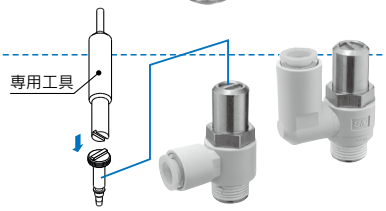
・製品のボタン部を押すことにより残圧を瞬時排気可能

対象機種

名称	シリーズ
ワンタッチ管継手付残圧排気弁付コントローラ	AS□□□1FE
ワンタッチ管継手付残圧排気弁	KE□

誤操作防止仕様

・不用意な手動操作を防止



対象機種

名称	シリーズ
マイナスドライバ調整用スピードコントローラ	AS□□□1F-D
タンパープルーフスピードコントローラ	AS□□□1F-T

中間停止・落下防止仕様

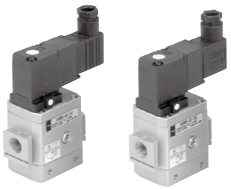
・シリンダの一時的な停止、速度制御を可能

対象機種

名称	シリーズ
パイロットチェック弁付スピードコントローラ	**ASP**
チェックバルブ	**AK**

飛び出し防止仕様

・給気を遮断し急速排気を可能
（ソフトスタートアップバルブ）
・2方向の流量制御が可能
（デュアルスピードコントローラ）



対象機種

名称	シリーズ
ソフトスタートアップバルブ	**AV**
デュアルスピードコントローラ	**ASD**

4 検出スイッチ

誤操作防止仕様

・暗証番号入力により不用意な手動操作を防止

センサ・アンプ一体型

名称	シリーズ
2色表示式高精度 デジタル圧力スイッチ	**ZSE30A(F)/ISE30A** **ZSE40A(F)/ISE40A**
薄形デジタル圧力スイッチ	**ZSE10(F)/ISE10**

センサ・アンプ分離型

名称	シリーズ
小型空気圧用圧力センサ	**PSE53□** **PSE54□**
微差圧センサ	**PSE55□**
汎用流体用圧力センサ	**PSE56□**
多チャンネルデジタル圧力センサコントロール	**PSE200**
2色表示式デジタル圧力センサコントロール	**PSE300**

残圧確認仕様

・シリンダ、生産ライン内の
残圧を目視確認が可能

対象機種

名称	シリーズ
エア用残圧表示器	**CB-97XH**

改訂内容

B版
- B10→B10(d)へ変更。
- 安全PLCを用いた配線図例を修正。
- 空圧機器推奨製品の見直し。
- 頁数24→20へ変更

TY