空気圧コントロールシステムにおけるインタロックシステムに関する研究

明治大学大学院　理工学研究科

２０１３年度

博士学位請求論文

Research on Interlock System in Pneumatic Control System

空気圧コントロールシステムにおけるインタロックシステムに関する研究

指導教員　杉　本　旭　教授

学位請求者　新領域創造専攻（安全系）

中　村　瑞　穂

目次

第 3 章　空気圧システムの故障解析

第 4 章　空気圧駆動システムの危険側故障を解消するインタロックの提案

第5章　空気圧駆動システムのインタロックによる安全確保とISO13849による安全関連系の整合性

付録

第１章　序論

1.1　本研究の背景

厚生労働省が 2013 年 5 月 24 日に公表した「平成 24 年度労働災害発生状況」[(1)] によると，全体として 2011 年度は死亡災害，死傷災害，重大災害いずれも 3 年連続の増加となっている．

全産業における死亡災害発生状況では死亡者数は全産業では 1,093 人, 前年度の 1,024 人に比べ 69 人（+6.7%）増加し 5 年前から増減を繰り返している．その中で，製造業は図 1-1 によると 199 人（前年比+17 人，+9.3%）である．

死傷災害発生状況では，全産業で死傷者数（死亡・休業 4 日以上）は 119,576 人，2011 年度の 117,958 人（東日本大震災を直接の原因とする災害を除く）に比べ 1,618 人（+1.4%）の増加となっている. その中で図 1-2 によると製造業では 28,291 人（前年比-166 人, -0.6%）である．事故の型（種類）は表 1-1 に示すように「はさまれ・巻き込まれ」，「転倒」の順に多くなっている．重大災害は全産業で 284 件，2011 年度に比べ 29 件増加しているが，図 1-3 に示すように製造業では 2011 年度に比べて 4 件減少しているが 2010 年からの 3 年間では大きな変化が見られない.

全体として労働災害の要因としては製造業全体の厳しい経営環境が安全衛生活動に影響を及ぼしていると見られる．

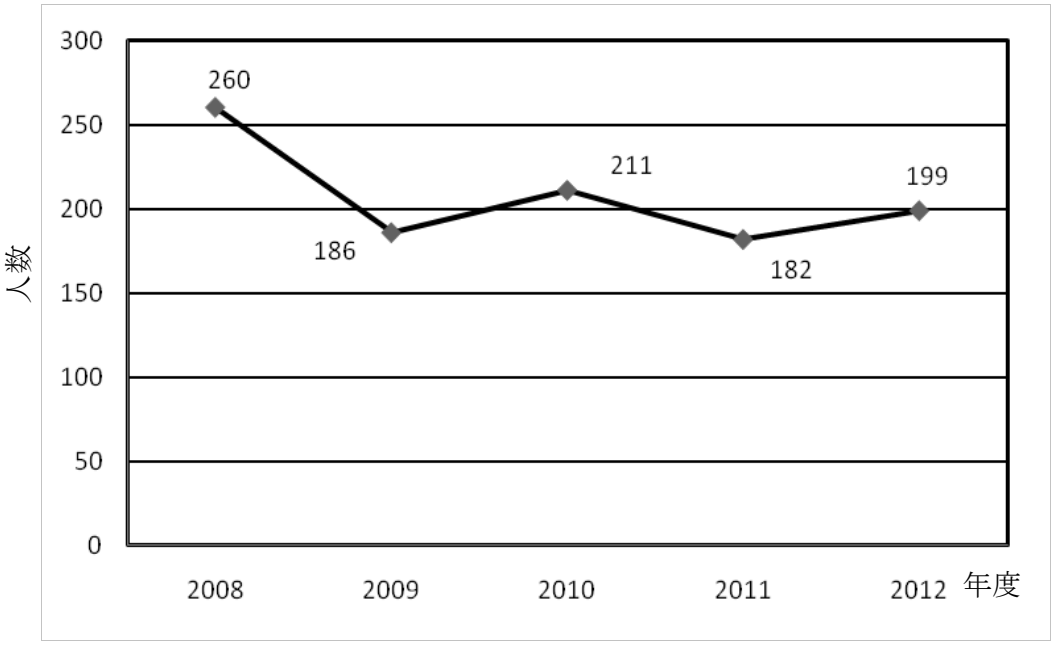


図 1-1　製造業における死亡災害発生状況（人）

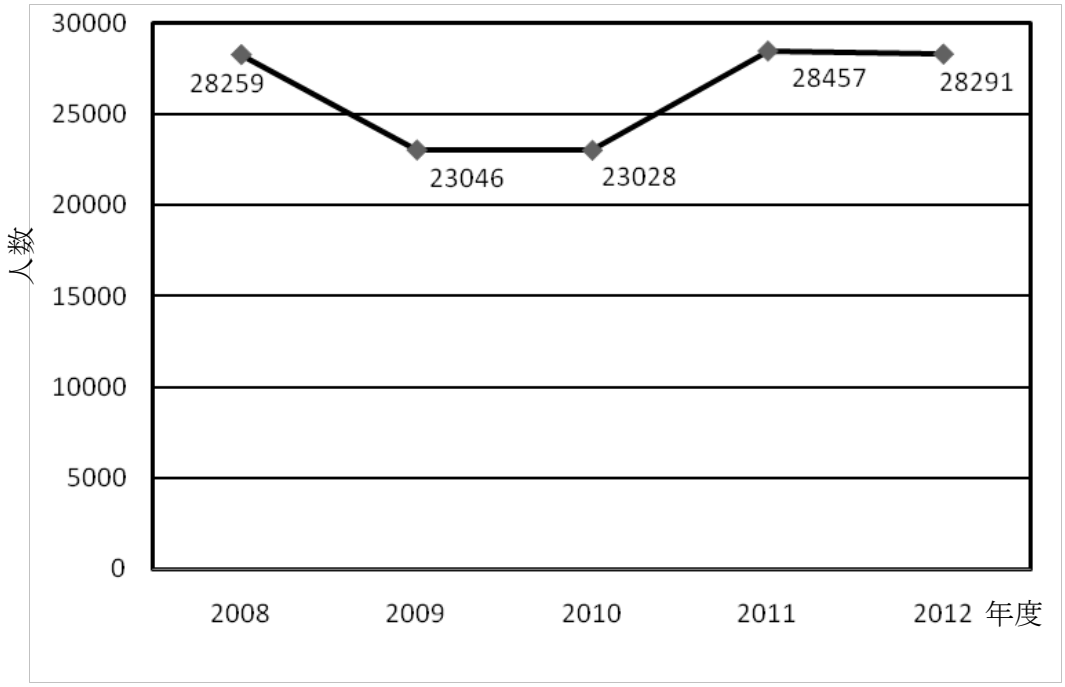


図 1-2　製造業における死傷災害発生状況の推移（人）

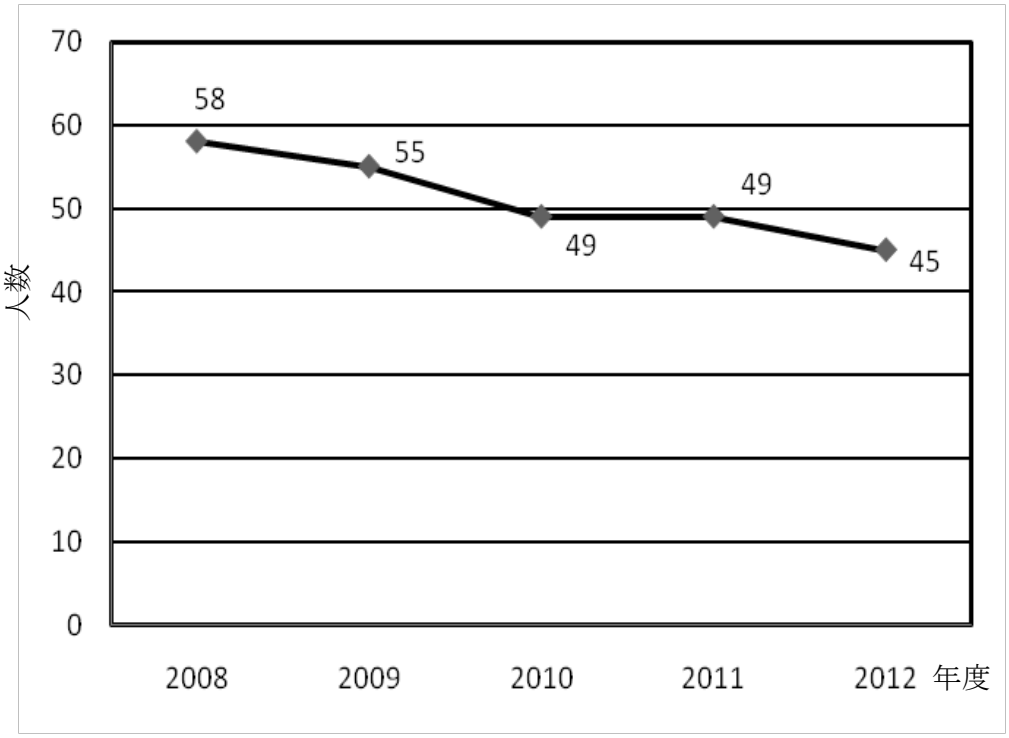


図 1-3　製造業における重大災害発生状況の推移

表 1-1　製造業における事故の型（種類）による死亡，死傷災害発生状況

事故の型	死亡災害発生状況（人）	死傷災害発生状況（人）
墜落・転落	38	2,926
転倒	7	4,869
激突	0	1,087
飛来・落下	14	2,378
崩壊・倒壊	18	687
激突され	6	1,095
はさまれ巻き込まれ	63	8,077
切れ・こすれ	1	3,098
踏抜き	0	40
おぼれ	1	1
高温・低温物との接触	6	872
有害物との接触	8	209
感電	4	38
爆発	6	54
破裂	3	27
火災	5	35
交通事故（道路）	13	352
交通事故（その他）	0	7
動作の反動無理な動作	0	2,313
その他	6	101
分類不能	0	25
合計	199	28,291

また，高圧ガス保安協会から発行されている「高圧ガス関係事故集計」[(2)] によると図 1-4 の高圧ガス事故統計集計表（災害）では 2008 年～2012 年度の 5 年間では 314 件から 458 件の間で増減しており，横倍な状態である．その中で表 1-2 による設備の事故で最も多いのは「劣化・腐食」であり，運転・操作では「誤操作，誤判断」によるものである．

現象別区分による分析（表 1-3）では「漏洩（噴出漏洩）」の災害が最も多い，「漏洩（噴出漏洩）」とは機器，配管，締結部開閉部，可動シールなどからの噴出・漏れを指している．さらに，機器や配管などの噴出漏洩の原因となるのは「劣化・腐食」によるものである．この「劣化・腐食」の防止には保全による維持活動と改善活動によって行われている．

高圧ガスを含む圧力システムの安全は過度の圧力からシステムの破壊･破裂を守るために，部品に対してのブリード（蒸気の放出）やベント（気体の放出）によって行われている．しかし，圧力供給源または高圧ガスの供給を遮断する機能が見られなく，過度な圧力が生じた時のブリード，ベントでは「噴出漏洩」の解決にならず，それで発生している災害が「事故（Accident：偶然の［予期できなかった］）出来事」とすることはできず安全システムとしては不足であると言える．

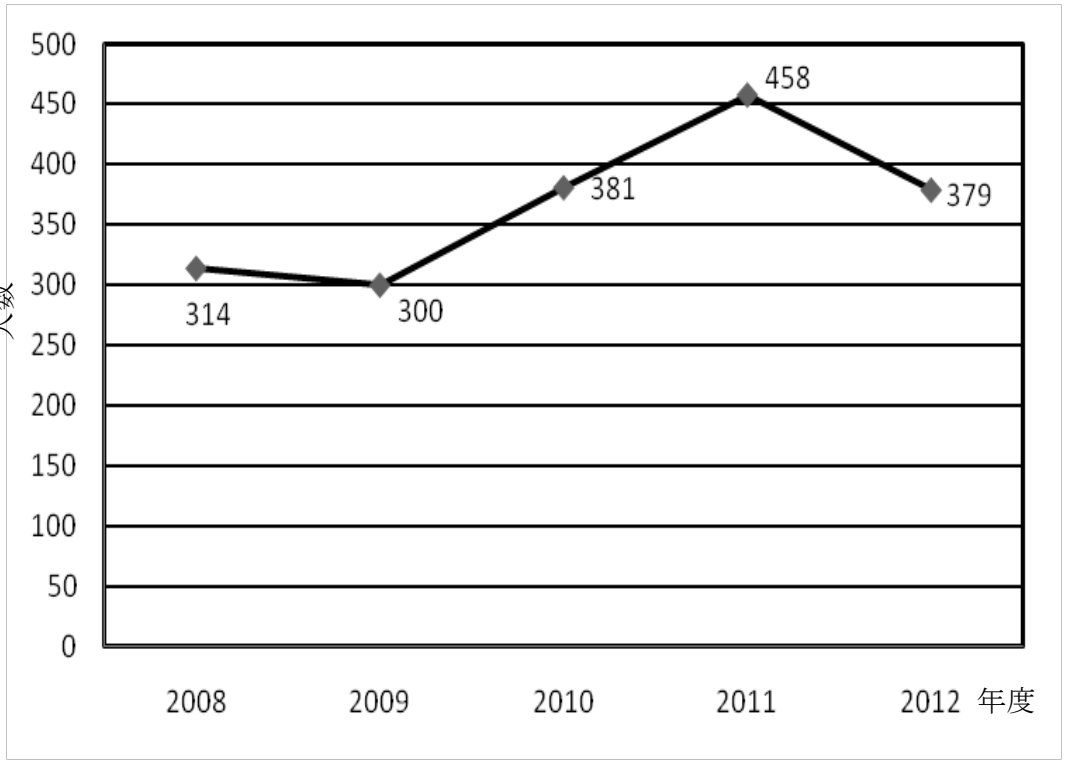


図 1-4 高圧ガス事故統計集計表（災害）

表 1-2　高圧ガス事故の原因別による分析（災害）

区分		原因	年度				
			2008	2009	2010	2011	2012
設備上（ハード）	設備の設計･構造不良	構造不良	7	7	16	19	27
		材質不良	2	1	0	17	7
		製作不良	15	17	28	10	7
	設備の維持管理不良	劣化・腐食	122	136	172	164	191
		点検不良	22	15	14	8	6
		誤作動	2	0	0	-	-
運転・操作上（ソフト）	管理･操作基準の不備	操作基準の不備	3	8	2	8	12
		情報提供の不備	1	2	3	1	0
		作業環境の不備	6	1	2	-	-
		責任管理体制の不備	2	0	0	-	-
	運転･工事に係るミス	誤操作	34	16	25	45	59
		誤判断	30	20	18		
		認知確認ミス	18	30	40	-	-

表 1-3　高圧ガス事故の現象別区分による分析（災害）

現象／年	2011 年（件）	2012 年（件）	2013 年（件）
爆発	6	7	3
火災	27	20	2
漏洩・噴出	373	158	94
破壊・破裂	44	316	5
その他	8	3	2
合計	458	379	106

一方，製造業では厳しい経営環境への対処方法としてFA化，ロボット化が進められている [(3)] 中で，空気圧システムが重要な要素として利用されている．

空気圧システムは工作機械，輸送機械，化学工業，造船，車両，自動車など製造業を中心に幅広く利用されている [(4)] ．利用にあたっては工場の全自動の自動化ラインのように人間と離れて使用される機器と医療機器などの人間と密接な状態で使用される機器があることから利用環境が機器により大きく異なる．そのため，空気圧システムを用いた機器を設計する際には，ISO12100-1 [(5)] では設計段階で「機械類の設計時に考慮すべき危険源」について同定し，保護方策を行うことが規定されている．しかし，空気圧システムを利用している機器は多種多様であり，中には人間が簡単に持ち運びできる機器もありユーザーの都合により簡単に使用環境を変えることが可能な機器が存在する．

設計段階での仕様は人間と離れた状態で使用されることで設計さている場合，ガードなどによる防護をしない場合が考えられる．つまり，設置環境の変化により機器の近くに人間が複数いる環境に変わった場合，空気圧コンポーネントや配管の破損，破裂による事故（人に危害を生ずる）に対処することができない．

空気圧システムの安全に関する国際規格は，A規格のISO12100-1 [(5)] ,2 [(6)] （機械類の安全原則），B規格ではISO13849-1 [(7)] （制御システムにおける安全関連部），ISO4414（空気圧システム通則） [(8)] によって規定されている．また，BIA報告 [(9)] ではアクチュエータの危険動作の防止による「安全」についてカテゴリBからカテゴリ 4 の空気圧回路を示している．

最近欧州規格として発行されたBS/EN764-7（火なし圧力容器の安全システム） [(10)] では安全システムを安全弁（減圧弁，リリーフ弁，ラプチャーディスクなど）による大気排出で構成することを規定している．

国際規格による空気圧システムの「安全」はシステムを構成する全ての空気圧コンポーネント（以降，コンポーネントと呼ぶ）はストレス・ストレングス・モデル [(11)] によ

る強度設計，安全弁（減圧弁，リリーフ弁，ラプチャーディスクなど）により外部への圧力排気, アクチュエータの危険動作, 残圧処理, ガードによる防護が規定されている．しかし，高圧ガス設備で発生している「噴出漏洩」が発生する可能性は十分あり得るが「噴出漏洩」の原因となる動力（圧縮空気）を遮断する機能は見られない．そのため，空気圧コンポーネントの危険側故障と圧力制御による危険側誤りが原因となる破損, 破裂による噴出漏洩に対しての「安全」が十分であるとは言いえない．もし，人間に密接した状態で使用される医療機器や空気圧工具などで過度な圧力上昇により空気圧コンポーネントが破裂して「噴出漏洩」されたときに高圧ガス設備の安全のように高圧の状態でベント（気体の放出）が行われた場合，事故が生ずる可能性が十分にある．

1.2　本研究の目的

本論文では，空気圧システムの圧力調整に伴う危険側誤りに関する調査と，そのリスクを解消するインタロックの実現可能性について論理的な検討を行い，その結果窓特性を有する監視によって空気圧駆動システムのフェールセーフ・インタロックシステム（以降，インタロックシステムと呼ぶ）が実現し得ることを示す．

インタロックシステムの機能と構成法等が国際規格で示されている安全関連系および安全システムとの関連性と相違点の評価を行い実用的なインタロックシステムとして空気圧システムへの適用について考察する．

1.3　本論文の構成

第 1 章では研究の背景，目的，構成，用語の定義と表現について説明する．第 2 章では空気圧システムの基本構造と関係する安全に関する国際規格について説明して，現状の空気圧システムの安全に関する問題点と安全システム（安全確認型，危険検出型）について考察している．

第 3 章では空気圧システムの構成例を用いて，システム構成する各種空気圧コンポーネント（13 種類）についてFMEA（Failure Mode and Effects Analysis）[(12)] を適用して故障モードの検討を行う．その結果，いくつかのコンポーネントで圧力が上昇する危険側の故障モードの存在が明らかとなった．また，低下する側の危険側の故障モードも多く存在する．そのため，空気圧システムの故障監視には，圧力の上昇と低下の両方を監視するのが有効であることを示している．さらに，FMEAの結果についてBIA-Report 6/97eとISO13849-2 の付属書B（空気圧システムの妥当性確認ツール）[(13)] との比較を行い故障モードの偏り等について検討を行い本質的な違い無いことを示した．

第 4 章では第 3 章における FMEA による空気圧システムの圧力調整に伴う危険側誤りに関する調査結果に基づき，そのリスクを解消するインタロックの実現可能性について論理的な検討を行い，その結果，窓特性を有する監視によってフェールセーフ・インタロックが実現し得ることを示す．

第 5 章ではインタロックシステムと国際規格で規定される安全関連系との整合性について検討を行う．そのため，本研究で提案するインタロックシステムの安全コンセプトを明らかにし，安全（確認）の原理に根拠を置く安全確保の妥当性について述べる．

インタロックシステムの構成条件について，そのリスク低減効果（停止による安全確保）について検討を行う．インタロックシステムを，機械安全に関する国際規格 IS12100-1，2 と制御安全に関する国際規格 ISO13849-1 の見方からの検討を行い，このインタロックシステムの国際規格との整合性について考察する．

インタロックシステムについて ISO13849-1 で規定される安全関連系としての評価を行う．インタロックシステムは，遮断弁を用いて，故障時，空気圧システムから切り離す構成である．これにより，空気圧コンポーネントの危険側故障はすべて，インタロックシステムの遮断構造に集約されると見ることができる．さらにフェールセーフな“窓監視”と故障時の遮断弁の“OFF 遮断”を採用することによって，危険側故障の影響を生じない理想的な安全関連系であることが期待される．これらの検討によって上記 2 つの安全の妥当性が整合可能であることを示そうとするものである．

最後に，第 6 章において，研究の結果をまとめ，今後の課題について述べる．

1.4 用語の定義と表現

NO.	用語	定義
1	安全	「受容できないリスクがないと（国際規格）」 「安全が確認されていること（論理的安全）」
2	危険	危険源および危険状態.
3	事故（危害）	身体または健康障害.
4	ブリード	蒸気化させて圧力容器から排出すること.
5	ベント	排出口という意味があり，圧力容器などから圧力を排出させること.
6	リスク	危害の発生確率と危害のひどさの組合せ.
7	危険側誤り	リスクを増加させるような（危険側故障の基になるような），制御による誤り.
8	危険側故障	リスクを増加させるような，機械類又はその動力供給における機能不良.

9	安全情報	安全を示す情報．状態を安全と安全でない場合とするとき，通常それを 2 値の論理変数，例えば S で表し，「安全」を S=1，「安全でない」を S=0 とする．
10	インタロック	特定の条件（一般にはガードが閉じていない場合）のもとで危険な機械機能の運転を防ぐことを目的とした機械装置，電気装置，または，その他の装置．
11	フェールセーフ（フェイルセイフ）	特定の障害モードが圧倒的に安全な方向にあるようなアイテムの設計特性．（IEC61508-4）
12	基本安全原則	安全に関わる制御システムにおいて意図する使用に対して適切な設計・製造であって，使用環境に対して信頼性を有するとともに，機械制御システムの安全性確保の基本原則として，機械の起動は動力の供給に基づき停止またはその遮断により，かつ，機械の停止時には予期しない起動の防止を有すること．（ISO13849-1，2）
13	安全（確認）の原理	安全（確認）の原理は，安全を維持する操作に危険側誤りが含まれる場合，安全を常時確認し，安全が確認できないときはシステムを停止するインタロックの必要性を主張する．
14	安全確認型システム	安全を直接抽出してそれを通報するシステムである．
15	危険検出型システム	危険を検出してその否定によって安全を通報するシステム．
16	安全制御	安全を示す信号に基づいて機械的出力が操作されるような安全の確認に基づく制御．
17	論理記号	論理式で用いられる記号．論理式 x∨y（論理和），x・y（論理積），¬x（否定），x+y（加算）や x∈｛1,0｝で用いられる記号∨や・，¬，+，∈は論理記号である．

18	論理式	例えば, 2 値の論理変数 x と y について論理和は x∨y で表し，論理積は xy，または x・y で表すものとする．加算演算は+の記号で表す．否定演算は¬の記号で表す．安全工学において論理式は論理変数として与えられる危険源に対して安全確保の方策とその結果を示す.
19	論理変数	論理値を変数とする．論理式 x∨y（論理和），x・y（論理積），¬x（否定），x+y（加算）や x∈{1,0}で用いられる変数 x や y は論理変数である．安全工学では危険源の有無，又はリスクの程度を論理変数で表す．論理変数は，危険区域か安全であるか否か，安全確保の機能は正常であるか否か，安全機能は規格に適合するか否か，管理は正しく守られているか否か，人または機械可動部の動作や挙動，などを示す.
20	論理値	論理変数がとる値.
21	FMEA（Failure Mode and Effects Analysis）	システムにおけるすべてのコンポーネントの故障モードとその影響（制御システムの安全関連部の出力への影響）を審査する方法である.
22	故障	要求される機能を遂行する能力がアイテムにこなくなること.
23	故障モード	機器や部品で発生する故障（機能停止型故障、機能低下型故障）の状態であり，故障の現象である.
24	リスクアセスメント	リスク分析及びリスク評価を含むすべてのプロセス.
25	リスク分析	機械の制限に関する仕様，危険源の同定及びリスク見積の組合せ.
26	リスク評価	リスク分析に基づき，リスク低減目標を達成したかどうかを判断すること.
27	窓監視	入力信号に対して上限と下限の検定機能を持たせるような監視.

28	検出	センサは‟検知の場“にしきい値を設けて，“検出信号”を生成する．検知信号はアナログ信号である．検知信号はアナログ信号である．検知信号はセンサの判断結果であるから 2 値信号である．
29	検知	センサは検知対象に対して，‟検知の場（視野）“をもつ．その検知可能な場を‟検知範囲”と呼ぶ．（IEC61496-1）
30	サージ圧	空気回路ではリリーフ弁の作動遅れや電磁切換弁の操作などにより油の流れが急激に変化する場合，流体の運動エネルギーが圧力エネルギーに変わり，圧力の急激な変動がおき，液体中を音波の伝搬速度で伝わり，空気圧回路の故障の原因となる恐れがある．この異常な圧力変動の最大値をサージ圧（surge pressure）という．
31	非対称故障モード特性	支配的な故障モードが事前に分かっていて，機械機能の変化を危険源が生じない側へ，その故障を導くように使用することができるものである．
32	対称誤りと非対称誤り	2 値信号｛1,0｝が 1 に誤らないときを非対称誤り信号，1 にも 0 にも誤るときを対称誤り信号とよぶ．1 側の誤りを生じない装置の特性は非対称誤り特性 1 側と 0 側のいずれにも誤りを生ずる場合の特性は対称誤り特性と呼ぶ．また，前者の特性を持つ機能を非対称誤り機能，後者の特性を対処誤り機能と呼ぶ.
33	能動的機能	機械の機能および人による操作によって実行される機能.
34	ノーマル・クローズシステム（構造）	安全状態が（通電状態として）連続的に確認されるシステム．安全確認型システムの構成方法．また，常に安全情報抽出の原理を満たす.

35	フォルトトレランス	障害発生時において要求機能を実行し続けるための機能ユニット能力．（ISO/IEC2382-14）
36	制御システムの安全関連部	入力信号に応答し，かつ，安全関連制御信号を生成する制御システムの部分またはその付属部分．制御システムに組み合わされた安全関連部は，安全関連信号の発生するところから，動力制御要素の出力生成までの過程を預かり，監視系を含む場合がある．
37	非安全関連部	システムの入力信号に応答し，安全には無関係に出力信号を生成する部分又は付属部分．非安全関連部には非対称誤りの出力特性を求めない．
38	独立性	（技術的独立性）複数のアイテムの正しい動作に影響するような，そのいかなる機構も存在しないこと．（人的独立性）知的，商業的および/または管理上の関与が存在しないこと．
39	安全コンセプト	安全システムを構成する際の“安全”に関する概念である．例えば危険側故障そのものの発生を防止する．
40	安全要件	安全コンセプトを達成するための中心となる機能を示す．
41	安全機能	故障がリスクの増加に直ちに繋がるような機械の機能．
42	危険側故障発生確率（MTTFd）	ISO13849-1 における安全関連系の評価基準であり確率で示されている．
43	カテゴリ	ISO13849-1 で示されている安全関連部の評価基準でB～4までの5段階によって構成されている．
44	安全防護	本質安全設計方策により合理的に除去できない危険源，又は十分に低減できないリスクから人を保護するための安全防護物の使用による保護方策．（ISO12100，ISO14119）
45	安全防護物	ガードまたは保護装置．（ISO12100）

46	意図する使用	使用上の指示事項中に提供された情報に基づく機械の使用.
47	機械類	連結された部品又は構成品の組合せで, そのうちの少なくとも一つは適切な機械アクチュエータ, 制御及び動力回路を備えて動くものであって, 特に材料の加工, 処理, 移動, 梱包といった特定の用途に合うように結合されたもの.
48	危険源	危害を引き起こす潜在的危険源.
49	残留リスク	保護方策を講じた後に残るリスク.
50	自動監視	動作要求が生じる前に安全機能の不具合を検出するために不具合を直ちに検出する. または周期的にチエックする機能.
51	非常停止	次のことを意図する機能. （1）人に対する危険源をまたは機械類若しくは行程中のワークへの損失を避けるか又は低減する. （2）使用者による（組織：安全作業手順, 監督, 作業許可システム;付加安全防護物の準備及び使用；保護具の使用；訓練）
52	保護方策	リスク低減を達成することを意図した方策であり, 設計者, 使用者によって実行される方策.
53	ポジティブな機械的結合	機械的構成部分が直接接触して, または合成要素を介して他の機械的構成部分に作用するような結合.
54	十分に吟味された安全原則	障害発生時のシステムの挙動を安全側に保つことを考慮した経験的安全性確保原則.（ISO13849-2）

第 1 章　参考文献

（1）「平成 25 年における労働災害発生状況（速報），厚生労働省労働基準局安全衛生部安全課，2013/7，http://www.mhlw.go.jp/bunya/roudoukijun/anzeneisei11/rousai-hassei/（参照日平成 25 年 11 月 23 日）

（2）「高圧ガス関係事故集計（平成 25 年 4 月現在）」，高圧ガス保安協会，2013/4，http://www.khk.or.jp/activities/incident_investigation/hpg_incident/statistics_material.html，（参照日平成 25 年 11 月 23 日）

（3）高橋徹著，“わかりやすい機械教室空気圧の基礎と応用”，東京電機大学出版局，pp.2，2005/5，第 7 版

（4）コガネイ・エアトロニクス研究会著，“新・知りたいエアトロニクス　改訂版”，ジャパンマシニスト社，pp.17，1993，初版

（5）ISO12100-1:2003,Safety of machinery-Basic concepts and general principles for design, Part 1：Basic terminology，methodology(2003)，International Organization for Standardization.

（6）ISO12100-2 : 2003，Safety of machinery-Basic concepts and general principles for design, Part 2：Technical principles(2003)，International Organization for Standardization.

（7）ISO13849-1:2006，Safety of machinery-Safety-related parts of control systems-Part 1:General principles for design(2006)，International Organization for Standardization.

（8）ISO4414:1998，Pneumatic fluid power-General rules and safety requirements for systems and their components(1998)，International Organization for Standardization.

（9）BIA-Report 6/97e，Categorized for safety-related control systems in accordance with EN954-1(1999)，HVBG.

（10）EN764-7:2002，Pressure equipment-Part7:Safety systems for unfired pressure equipment(2002)，European Standard.

（11）田村泰彦，飯塚悦功：“不具合に関する設計知識の運用に関する研究－ストレス-ストレングスモデルによる知識獲得 -”，品質，Vol.31,No.1(2001),pp168-180

（12）田中健次著，“技術者がはじめて学ぶ　入門信頼性”，日科技連，pp.136，2008/12，初版

（13）ISO13849-2:2003，Safety of machinery-Safety-related parts of control systems-Part 2:Validation(2003)，International Organization for Standardization.

第 2 章　空気圧システムの基本構造と関連する安全規格・技術

2.1　はじめに

本章では，第2.2節では空気圧システムの概念および基本構造を述べ，一緒に各種コンポーネントの機能，図記号による表現と動作プロセスについて述べ，本研究で用いる空気圧システムの代表的構成例を示す．第2.3節では国際安全規格の概要と特徴，ISO/IEC Guide51について説明し，国際安全規格では安全をリスクで表しているためリスク低減の方法論について説明する．第2.4節ではISO12100-1，2の概要と空気圧システムの設計または仕様書作成上での安全性確保の基本的要求事項について述べる．第2.5節ではISO13849-1（制御システムの安全関連部：設計原則）について説明する．第2.6節ではISO13849-2（制御システムの安全関連部：妥当性確認）の空気圧コンポーネントの制御装置の特別要求事項，実績のある安全原則，油空圧コンポーネントにおける基本安全原則と適用例について説明する．第2.7節ではISO4414（空気圧システム通則）の安全に関する要求事項について，第2.8節では空気圧コンポーネントおよび制御装置の特別要求事項について説明する．第2.9節では安全システムおよび安全（確認）の原理について説明する．

本章では本研究を行うのに必要な空気圧システムの概要と関係する国際安全規格および空気圧システムに関係する国際規格について説明を行い，空気圧システムにおける安全に関する問題点と課題および関係する国際規格について考察している．

2.2　空気圧システムの概念と基本的構造

2.2.1　空気圧システムの概念

空気圧システムでは動力源として電気的エネルギー（信号を含む）を用いて圧縮空気を発生させる．この圧縮空気は配管を経由して制御部で圧力，方向，流量を外部から別の電気的エネルギーまたは手動弁，すなわち，信号のエネルギーで制御されて出力される．この制御には例えば圧力制御弁，方向制御弁，流量制御弁など各種制御弁が使われて，制御の結果は作動部の空気圧アクチュエータによりシステム外部への機械的出力エネルギーとなる [(1)]．(図2.1参照)

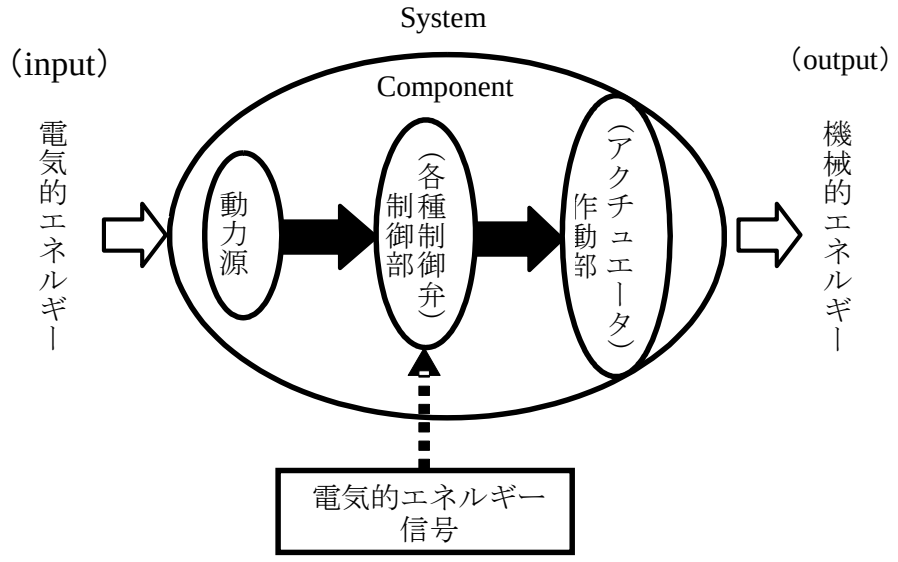


図 2.1　空気圧システムの概念

2.2.2　空気圧システムの機能と構成

空気圧システムの構成は図2.2の機能ブロック [2], [3] に示すとおりに①～③の3つで構成されている．その中で，①動力供給部はコンプレッサでは外気から吸い込んだ空気から圧縮空気を生成する [4]．圧縮 空気は高温であるためエアクーラで冷却され [5]，圧縮空気中の水分や塵埃などをドレンセパレータで分離する [6]．この圧縮空気をタンクに蓄積し，アクチュエータなどの動作により発生する急な負荷の変動に対処する [7]．また，圧縮空気は高温，高湿であるため空気圧コンポーネントの故障の原因となるためドライヤで乾燥させている [8]．①動力供給部は一般的な空気圧システムではユーティリティとしている．

②の動力調整部では①動力供給部から供給された圧縮空気中の水分，塵埃，油などをフィルタ [9] で分離，清浄し，レギュレータ [10] で③の駆動系で動作させるアクチュエータで作業を行うのに必要な圧力に制御される．さらに，ルブリケータでは圧縮空気中に潤滑油を噴霧して駆動系のコンポーネント(アクチュエータ, スピードコントローラ, 電磁弁，配管等）の潤滑を行う [11]．

③の駆動系では②動力供給部から供給された圧縮空気を方向制御弁でアクチュエータが作業する方向に圧縮空気を流す [12]．さらに，スピードコントローラで圧縮空気の流量を制御してアクチュエータの速度制御を行っている [13]．最後に，アクチュエータにより仕事を行う [14]．図2.2に基づく空気圧システムの構成例を図2.3に示す．また，表2.1に図2.3を構成している各種空気圧コンポーネントとその機能を示す.

空気圧システムでは, 機械的エネルギーから流体圧エネルギーの動力源を生成するためのエネルギー変換は①動力供給部のコンプレッサ（動力源）により行われ，その他のコンポーネントはエネルギーを伝達する部分である. ②動力調整部は流体圧エネルギーを調整する部分である. ③駆動系は流体圧エネルギーを再び機械的エネルギーとするためのエネルギー変換部分がアクチュエータであり, このようにエネルギー変換が行われて空気圧システムは運転される.

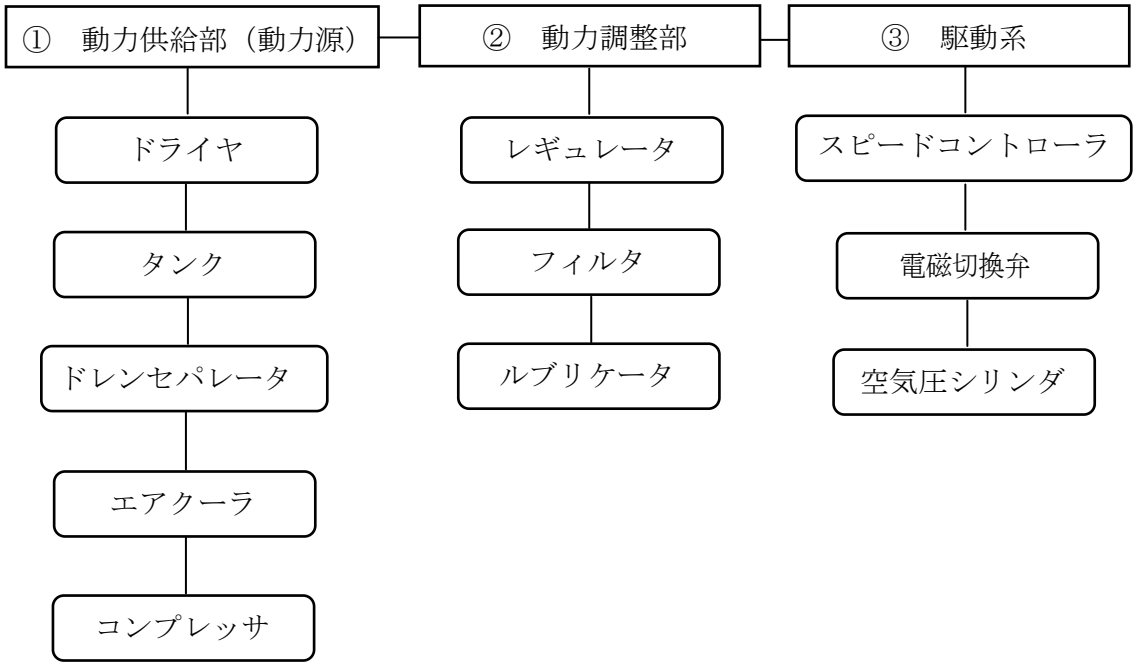


図 2.2　空気圧システムの機能ブロック図

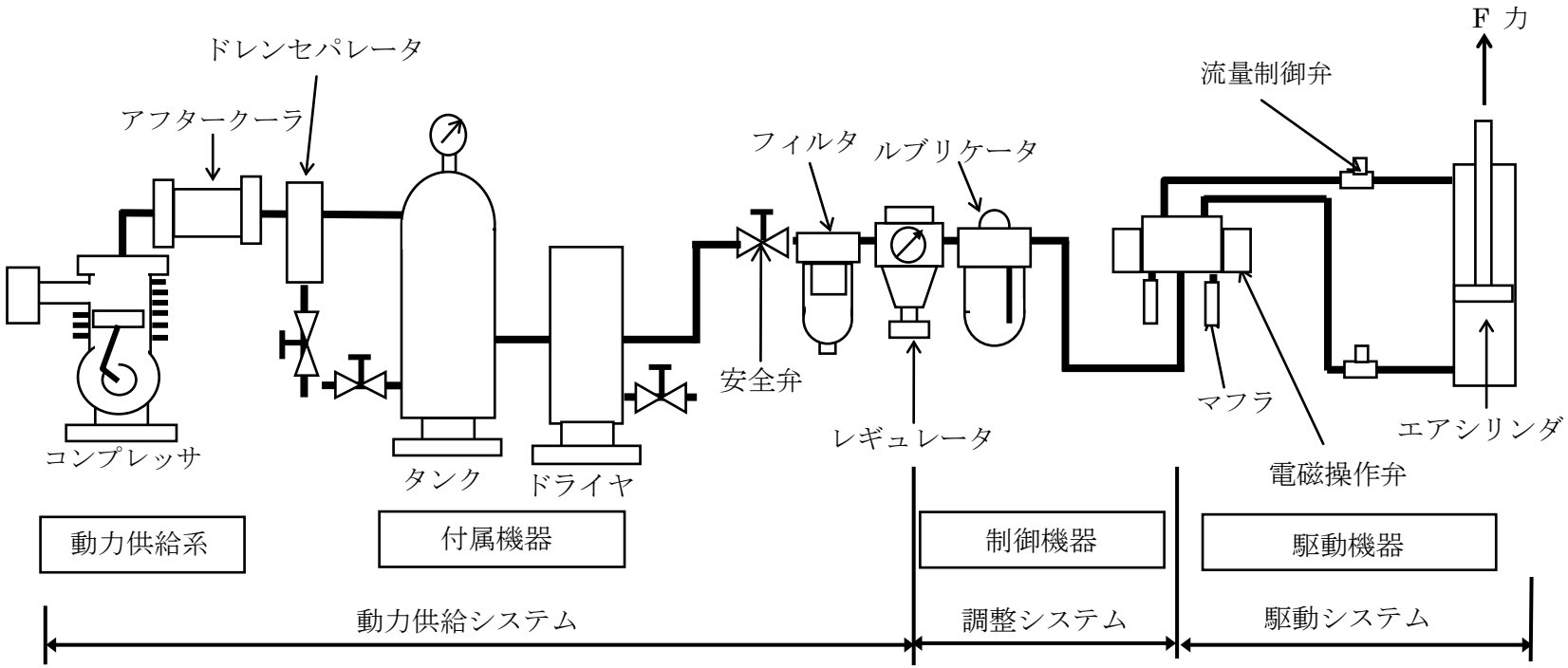


図 2.3　空気圧システムの構成例 [15]

表2.1　空気圧コンポーネントと機能

コンポーネント	機能
コンプレッサ	空気を吸入して圧力を加えて空気圧制御システムの動力である圧縮空気をつくりだす
アフタークーラ	コンプレッサが吐出した圧縮空気を冷却する熱交換器
ドレンセパレータ	圧縮空気中に含んだドレンを分離する
タンク	動力源である圧縮空気を蓄える容器
ドライヤ	圧縮空気中に含む水分を除き乾燥した圧縮空気を得る機器
フィルタ	空気圧回路の途中に取付，ドレン及び微細な固形物を遠心力やろ過作用などで分離除去する機器
レギュレータ	二次側（出口）の圧力を，より低い設定値に変更する場合，その設定を用意にする目的のバルブ
ルブリケータ	油を霧状にして空気の流れに自動的に送り込む，空気圧機器への自動給油機器
マフラ	排気音を減少させる機器
方向制御弁	流れの方向を制御するバルブの総称
流量制御弁	流体の流量を制御するバルブでアクチュエータの速度制御に用いる
エアシリンダ	流体エネルギー圧（油圧・圧縮空気）を用いて機械的に仕事をする機器
リリーフ弁	回路内の圧力を設定値に保持するために，流体の一部又は全部を逃がす圧力制御弁

2.2.3　空気圧システムの図記号による表現

図2.4は図2.3を空気圧システムで一般的に利用される図記号（JIS記号）を用いて示してある．また，図2.5に同システムの写真を示す．写真についてはコンプレッサからフィルタまでの機器についてはユーティリティであるため写真には写ってはいない．

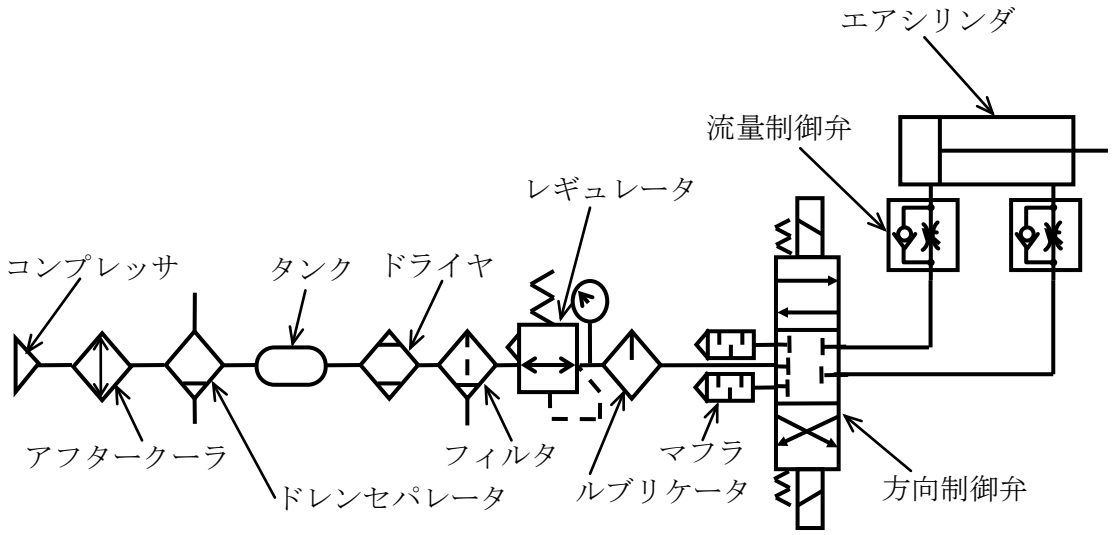


図 2.4　図 2.3 の空気圧システムの回路図（図記号）による表現 [16]

図2.5　空気圧システムの写真（例）

2.2.4　現状の空気圧システムにおける圧力制御に関する安全システム

図2.6は現状の空気圧システムにおける安全システムを示している．空気圧システムにおける圧力調整はレギュレータによって行われている．ここで安全システムはレギュレータ（M），安全弁（m1），リリーフ弁（m2），減圧弁（m3），ラプチャーディスバルブ（m4）によって構成されている．レギュレータを始めとする5つの空気圧コンポーネントはすべて外部への排気（リリーフ）することにより高圧空気の出力を防いでいる．また，図2.6のシステムを構成するコンポーネントはISO13849-1のカテゴリ評価を行う場合にはカテゴリB程度の評価であるためコンポーネントの信頼性に依存することになる．

そのため，5つのコンポーネントの全てに危険側故障が生じた場合，高圧空気の供給が継続されてしまい噴出や部品飛来などにより人に危害を与える可能性がある．

つまり，安全システム自身の故障がリスク増大の原因となるリスクが残ることになるため安全システムとしては不足していると見ることができる．安全システムとして不足な点は高圧空気がリスクとして残るため，これを遮断する動力遮断構造が存在しないことである．

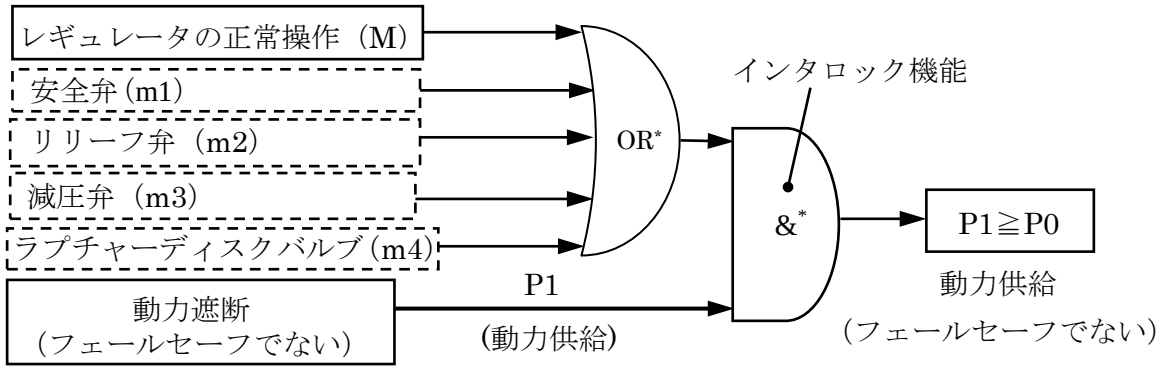


図 2.6　現状の空気圧システムにおける圧力制御に関する安全システム

2.3　国際安全規格の概要とリスク低減方法

2.3.1　国際安全規格の概要と特徴

日本では JIS（日本工業規格），米国では（ANSI），英国では（BS），ドイツでは（DIN）など世界の国々はそれぞれ，自国の国家規格を持っているが，これらの規格が原則整合化／統一化されていく流れになっており，国際規格 ISO（International Organization for Standardization，国際標準化機構）や IEC（International Electrotechnical Commission，国際電気標準会議）などによって行われている．この目的は物及びサービスの国際貿易を容易にし，かつ，知的，科学的，技術的及び経済的な活動をより拡大するために標準化を図ることである．

その中で機械安全の分野の規格については ISO，IEC によって発行されているが，EU 指令（機械指令，LVD 指令，EMC 指令など欧州域内の法律）を背景とした EN（European Standard：欧州規格）により原案が開発されている．開発された ISO，IEC 国際安全規格には（1）～（4）の共通の特徴がある．

（1）安全規格を 3 段階に分け階層化
（2）技術基準
（3）リスクアセスメントによる安全性評価
（4）3 ステップメソッドによるリスク低減方策

（1）は図 2.7 に示すように ISO，IEC 国際安全規格には A 規格（基本安全規格），B 規格（グループ安全規格），C 規格（個別安全規格）の 3 段階で階層的に構成されている．具体的な内容は 2.3.2 項で説明する．

（2）は ISO，IEC では規格の技術基準を性能規定としているが，JIS では仕様規定となっている．性能規定とは対象となる製品に必要な実用性（寿命，信頼性等）を定性的，定量的に表現した規定である．さらに，仕様規定とは対象となる製品の構造，形状，寸法，材料，外観等の項目を含んだ，設計または記述的特性を含んだ規定である．

（3）はリスクアセスメントの実施によりリスク分析，リスク評価を行いリスク低減の判定を行う作業の実施が規定されており，従来の JIS にはこのような考え方はなかった．

（4）は 3 ステップメソッドとは本質安全設計方策，安全防護策，使用上の情報の 3 分類されており，優先順位付けがなされている．

ISO/IEC Guide 51 [17] は規格に安全に関する規定を導入するためのガイドラインであり，（1）～（4）はこの規格で規定されている．すなわち，多くの国際安全規格は，このガイドをベースとして作成されていると言える．また，（1）～（4）の特徴はEN414（Safety

of machinery : Rules for the drafting and presentation of safety standards）の中でも規定されている.

2.3.2 ISO/IEC Guide51

ISO/IEC Guide51 は, 規格に安全に関する規定を導入するためのガイドラインである. 正式名称は Safety aspects-Guidelines for their inclusion in standards であり, ISO（International Organization for Standardization : 国際標準化機構）と IEC（**I**nternational **E**lectrotechnical **Co**mmission : 国際電気標準会議）の両組織において共同で開発, 発行した国際規格である. この規格では安全やリスクなどの概念や安全性を達成するための方法が示されているのと, 安全規格を作成する方法や既存の規格に安全規定を導入するために必要な一般的作業手順が示されており, 表 2.2 にこの規格の構成を示す.

表 2.2　ISO/IEC Guide51 の構成 [18]

序文
1. 適用範囲
2. 引用規格
3. 定義
4. 「安全」および「安全な」という用語の使用
5. 安全という概念
6. 許容可能なリスクの達成
7. 規格における安全側面
参考文献

この規格で安全はリスクで定義されており, リスクアセスメントとリスク低減方策により安全を確保することを規定しており, 規格の構成は図 2.7 に示すように基本安全規格（A 規格）, グループ安全規格（B 規格）, 個別機械安全規格（C 規格）のように階層構造になっている.

基本安全規格（A 規格）は, 設計のための基本原則, 用語などを定める規格で, すべての機械類に適用できる基本安全規格である.

グループ安全規格（B 規格）はシステム安全規格, インタロック規格, 空気圧システム通則などを定める規格で, 広範囲の機械類にわたって使用される安全面または安全関連装置の一種を取扱うグループ安全規格である.

個別機械安全規格（C 規格）は，工作機械，プレス機械，産業用ロボットなど個別の機械を対象として取扱う製品安全規格である．

このように体系化されているためすべての全体の整合性や統一性を持たせることができるため，すべての機械や新しい機械の安全を対象にでき，新しい安全技術を取り込むことができる．

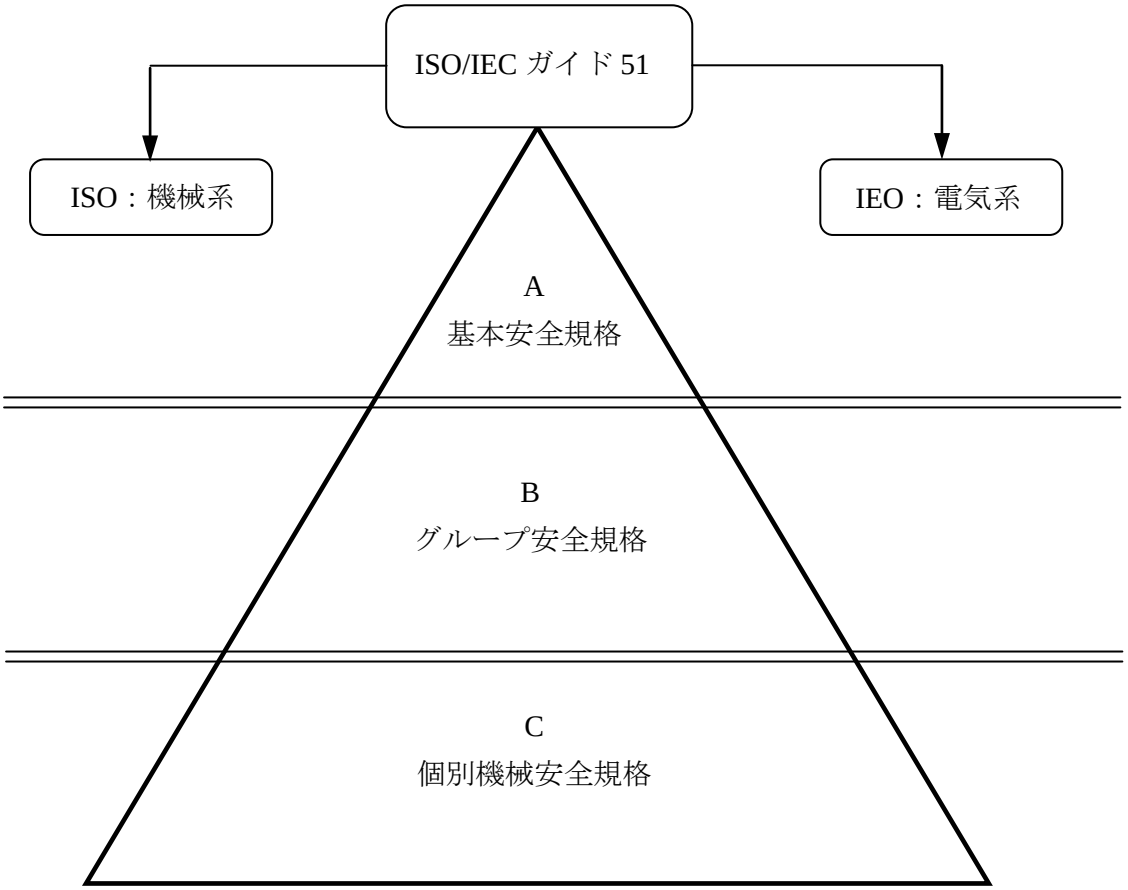


図 2.7 国際安全規格の階層化構成

2.3.3 安全の定義と ALARP の原理

ISO/IEC Guide51 によると安全（Safety）は「受け入れ不可能なリスクが無い状態（freedom from unacceptable risk)」と定義されている．リスクとは「危害の発生確率およびその危害の程度の組合せ」[19] で定義されておりRをリスク，Pを危害の発生確率，Sを危害の程度としたときに（2.1）式に示すように表すことができる．

リスク(R)=危害の発生確率(P)･危害の程度(S)　　(2.1)

（2.1）式で“･”は，組合せを表しており，必ずしも掛け算ではなく，RはPとSとの関数（f）であることを表している．そのため，安全を“受容できないリスクがないこと”と定義している．さらに，絶対安全があり得ないことが主張されており，安全を“受容できないリスクがない”または“許容可能なリスク”，“受け入れ可能なリスク”として規定している．つまり，「リスクが少ないから安全である」と規定している[19]．

図 2.7 に用語上で定まるリスクの存在形態を示す. 3 辺 ABC で示す三角形はリスクを表すものとして，この面積が小さくなるほどリスクが小さいとする．受け入れ可能なリスク Ra は許容可能なリスク Rt に比較してリスクは小さいとしている. ￢の記号は否定を表す. 受け入れ可能なリスク Ra と受け入れ不可能なリスク￢Ra は共通領域を有し得ないから両者の間には必ず隙間を必要とする．すなわち，両者のいずれであるか否かの不明が含まれる．同様に許容可能なリスク Rt と許容不可能なリスク￢Rt の間には必ず隙間を必要とする．以上を図 2.8 の面積で比較して，それを大小関係で表すと式（2.2）と（2.3）の通りである．

広く受け入れ可能なリスク(Ra)＜広く受け入れ不可能な(￢Ra)　　(2.2)

許容可能なリスク(Rt)＜許容不可能なリスク(￢Rt)　　(2.3)

安全は「受け入れ不可能なリスク（￢Ra）の不在」と定義される．よって，“許容不可能なリスク”レベルは“受け入れ不可能なリスク”のレベルより小さいことになり，式（2.4）で示される．

許容不可能なリスク(￢Rt)≦受け入れ不可能なリスク(￢Ra)　　(2.4)

よって，国際的には安全の定義（￢Ra）より小さいリスク，すなわち，“許容不可能なリスク（￢Rt）の中で，許容可能なリスク Rt を求めて要求事故を定めることになる．

許容可能なリスク(Rt)＜許容不可能なリスク(¬Rt)≦安全の定義(¬Ra)　　(2.5)

図 2.8 は“受け入れ可能なリスク”領域 Ra と“受け入れ不可能なリスク”領域¬Ra の隙間に“許容可能なリスク”の領域と“許容不可能なリスク”の領域を取ってその許容可能条件を定めた例で，ALARP 原理と呼ばれる．許容可能なリスク領域の利用には例えば（1）～（2）の制限が適用される．

（1）リスクが ALARP の領域にあることを論証するだけでは許容可能とはならない．
（2）ALARP であることの論証は例えば以下による．
・現状で最も利用できる規格と慣例の適用（state of arts）
・コスト／ベネフィット分析および寿命上の有効性の導入

図 2.9 は各種技術分野における機能上の安全性確保に関する規格IEC61508-5 : 1995 で示され，その後鉄道システムの生産性および安全性の評価への適用参照例として示される．また，日本でよく行われているリスクアセスメント上の安全の手抜き（リスクアセスメントを実施すれば，安全性確保上では見逃してはならないリスク，または分かっているのに故意に見逃すようなリスク）には，本来このALARPの原理による説明が求められる[20]．

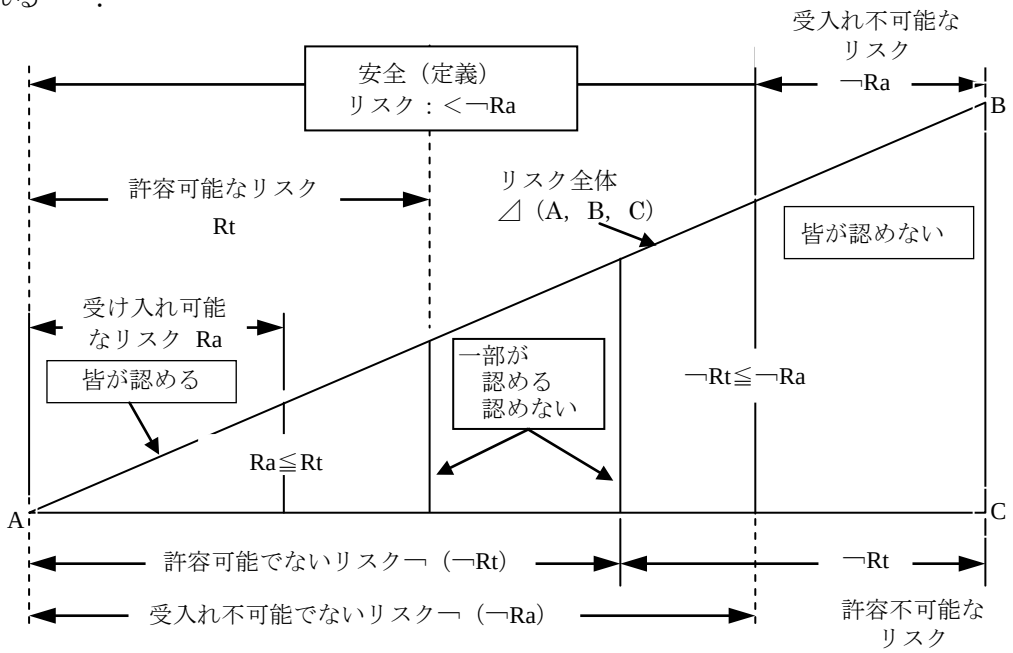


図 2.8　安全の定義と許容可能なリスク（¬の記号は否定を表す）

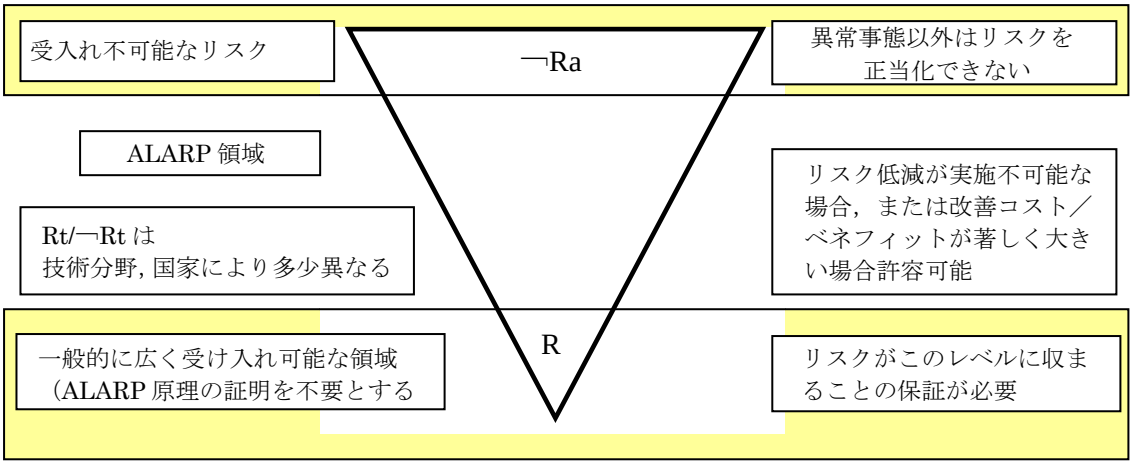


図 2.9　ALARP（As Low As Reasonably Practicable）原理：IEC61508-5:1995
（合理的に実施可能なリスクの低減）

2.3.4　リスク低減のための方法論

リスクアセスメントの実施とリスク低減方策（保護方策）については，ISO/IEC Guide51 中でリスクアセスメントの手順(図 2.10)とリスク低減方策は保護方策(図 2.11)が規定されている．図 2.10 のリスクアセスメントのプロセスの中で最も重要な作業は「ハザードの特定」と「リスク低減方策の妥当性確認」である．しかし，リスクアセスメントを実施して許容できないリスクが明らかになった場合に許容可能なレベルまでリスク低減を図らなくてはならない．リスク低減を達成するために必要とされる手段である保護方策を図 2.11 に示す．保護方策は設計側と使用側に分類されている．設計側の方策には本質安全設計，安全防護策，使用上の情報の提示の 3 つがある．使用側では追加保護装置，訓練，保護具，組織の 4 つがある．

設計側では本質安全設計によりリスクを可能な限り低減し，残留リスクが存在する場合に保護装置を適用する．さらに，保護装置を用いても設計上では残留リスクの低減がなされなかった場合には，このリスクについて使用者に対して提示する．このようにリスク低減は図 2.12 にしたがって，リスクアセスメントの反復を行ってリスク低減を図り安全（許容リスクレベルまたは受入れ可能なリスク）を達成する．

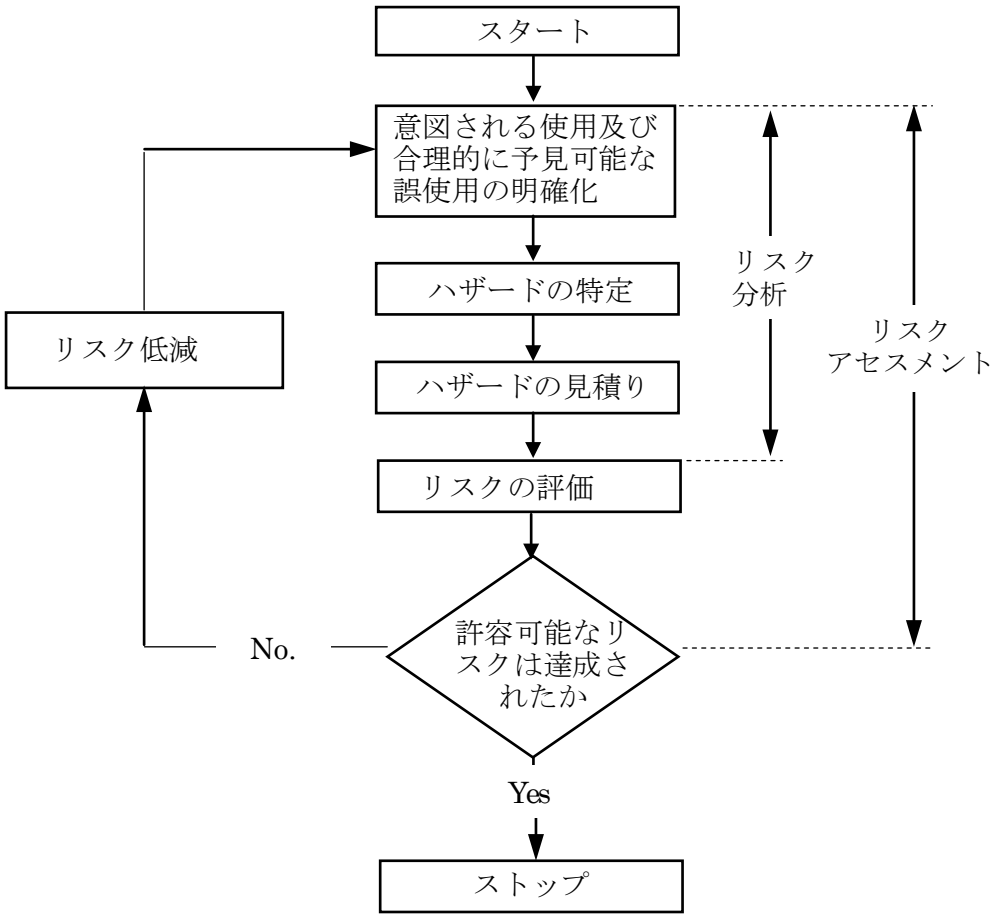


図 2.10　ISO/IEC Guide51 で示されるリスク低減プロセス

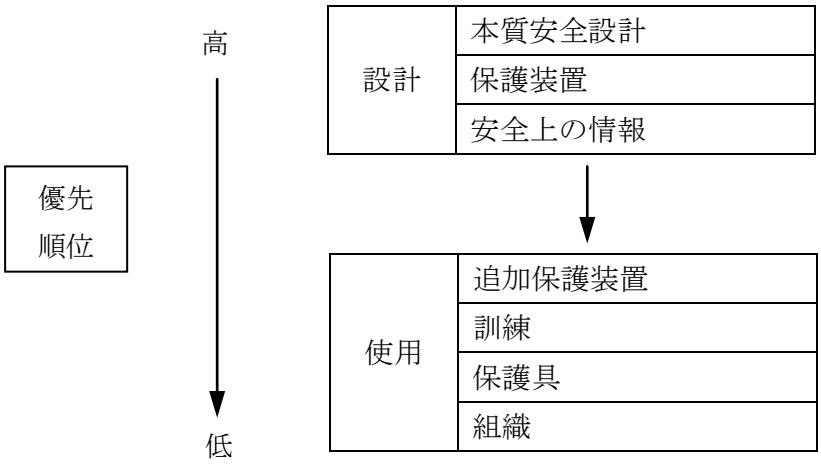


図 2.11 リスク低減方策と優先順位

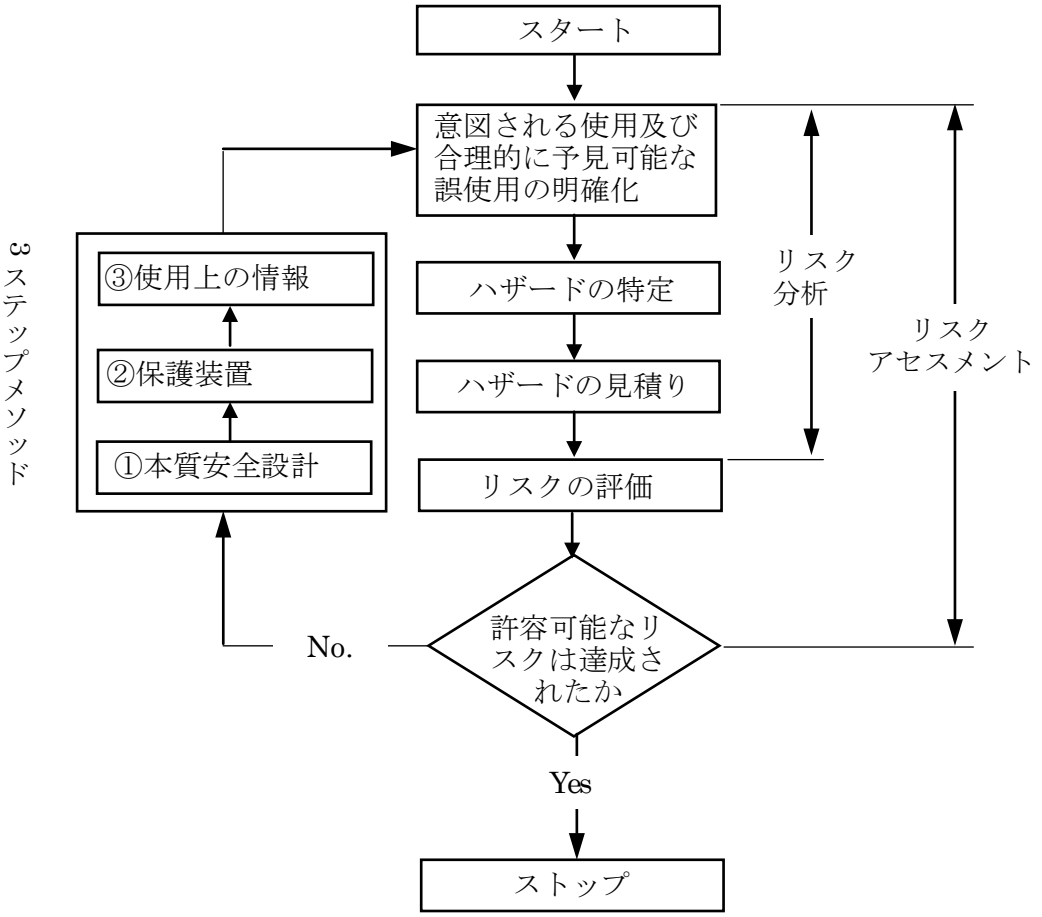


図 2.12　リスクアセスメント及びリスク低減の反復プロセス

2.4　ISO12100（機械類の安全性，設計のための基本概念，一般原則）

2.4.1　ISO12100 の概要

ISO12100（機械類の安全性，設計のための基本概念，一般原則）は第 1 部（以降，ISO12100-1 とする）[21]，第 2 部（以降，ISO12100-2 とする）[22] からなるA規格であり，第 1 部では機械類に関する安全規格の作成上で基本となる用語の概念と，安全性確保の方法に対する考え方が示されている．第 2 部では現在の技術として利用可能な技術により，第 1 部の概念や考え方を実現するための助言を与える内容である．ISO12100-2 で示されているすべての機械類の安全方策は図 2.13 に示すように本質安全設計，安全防護，追加安全方策，使用上の情報によって構成されている．

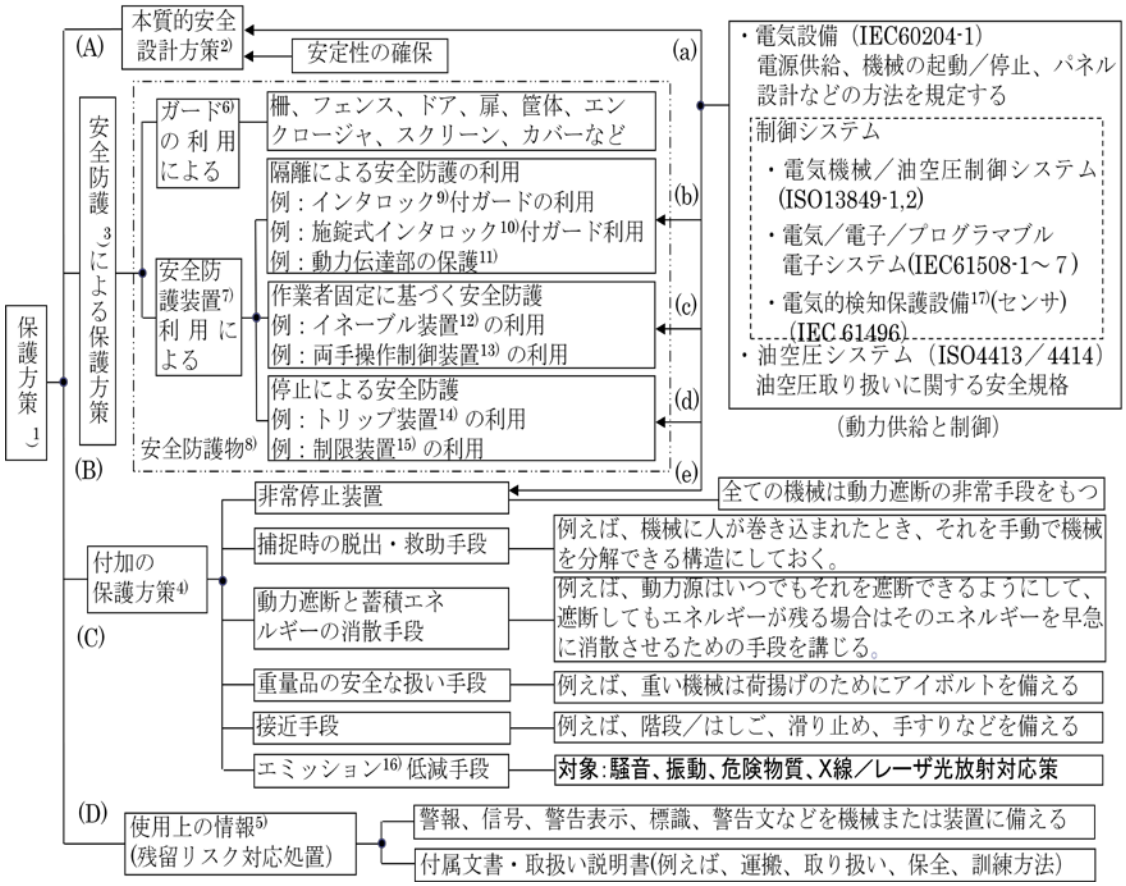


図 2.13　機械の安全設計を規定する国際安全規格ISO12100 の規格体系 [23]

2.4.2　空気圧システムの設計または仕様書作成上の基本的要求事項

国際規格 ISO12100-2 では油空圧制御システムの設計または仕様書作成上の基本的要求事項として以下が示される.

(1) 回路の最大許容圧力を超過することがないこと.（例：圧力制限装置の使用）

(2) サージ圧もしくは圧力増加，圧力の喪失もしくは降下，真空度の喪失により危険源を生じないこと.

(3) 漏れまたは構成部品の故障により危険な流体の噴出，またはホースのむちのような突然の動きを生じないこと.

（4）空気レシーバ，空気貯蔵器または同様の容器(液体／空気-アキュムレータ等)は，これらの要素に対する設計規則に適合していること．
（5）設備の全要素，特に管およびホースは，有害な外部の影響から保護されていること．
（6）貯蔵器および同様の容器（例：ガス封入のアキュムレータ）は，機械の動力供給を遮断した場合に可能な限り自動的に減圧できるようにし，これが不可能な場合，その遮断手段または局部的減圧および圧力表示の手段を設けること．
（7）機械を動力供給から遮断した後でも圧力を維持する全ての要素は，明確に同定できる排出装置を設け，かつ，機械の設定（段取り）または保守作業にかかる前に，これらの要素の減圧が必要であることについて注意喚起の警告ラベルを表示すること．
（8）動力源の ON/OFF，動力源の低下，動力源の遮断または再投入により意図的または不意の危険源を生じない．

2.5 ISO13849-1（制御システムの安全関連部：設計の一般原則）

ISO13849（制御システムの安全関連部 Safety related parts/control system：SRP/CS）は第 1 部，第 2 部から構成されている B 規格である．第 1 部では機械の安全に関する制御部分の設計手順が示され，カテゴリによるリスクの大きさの評価方法が説明されている．第 2 部では，各種制御要素で配慮すべき故障モードが示されている．

ISO13849-1 [(24)] は制御システムの安全関連部（SRP/CS）の設計及び組込みの原則（ソフトウエアの設計を含む）に関する安全性要求事項を規定し，SRP/CSに対し，構築されるべき安全機能の要求性能レベルを含む性能を規定する．また，この規格は，使用する技術，エネルギーの種類（電気，空気圧，油圧，機械的エネルギー等）を問わず，全ての機械類の制御システムの安全関連部に適用することが可能である．

制御システムの安全関連部（SRP/CS）はISO12100 とISO14121 [(25)] の原則を満足して設計・構成されている必要がある．そのため図 2.14 は制御システムの安全関連部の設計プロセスを示す．基本的にはISO13849-1 もISO12100 と同じように安全の定義がISOの考え方なので制御システムの安全関連部はリスク低減のためであることと言える．

図 2.14 のステップ 2 までは ISO12100 および ISO14121 と同様のステップであるが，ステップ 3 から制御システムの安全関連部の構成に入る．ステップ 3 で安全機能および特性を定める．安全機能については表 2.3 に示すように主に機械・システムの起動，停止，緊急停止などの機能について規定されている．さらに，この機能は ISO12100-2 から引用されている機能もある．

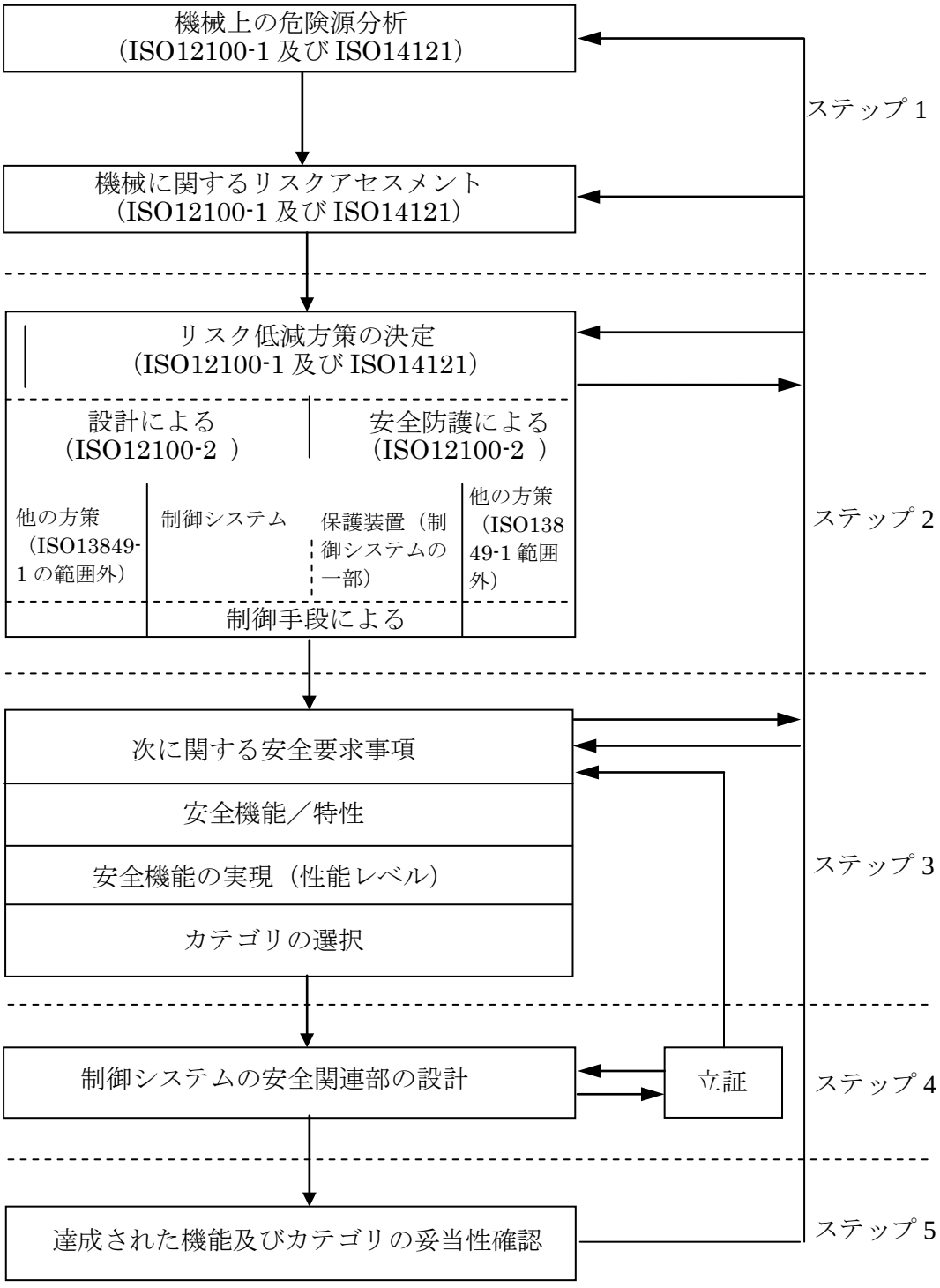


図 2.14　ISO13849-1 に示される制御システムの安全関連部の設計プロセス[26]

表 2.3　代表的な安全機能

安全機能／特性	機能の内容
安全防護装置の安全関連停止機能	安全防護物や保護装置により停止する機能である.
手動リセット機能	安全防護物や保護装置が停止命令により始動した後, 再起動のための安全条件が存在するまでその停止を維持する機能である.
起動／再起動機能	機械・システムの再起動機能で再起動時に危険状態例えば（工作機械作業でオペレータが加工物を調整している際に機械が再起動することを防止する機能.
ローカルコントロール機能	携帯式制御装置, ペンダントなどのようにローカル（局所）で制御される機能であり，主制御との切替えで危険状態が生じてはならない機能である.
ミューティング機能	SRP/CS による安全機能の一時停止を可能にする機能である.
ホールド・ツゥ・ラン機能	アクチュエータを作動させている間に限り，危険な機械機能の起動開始指令を出し，かつ維持する機能.
イネーブル制御機能	起動制御に連続して用いる調整または保全などの補足的な手動操作機能.
予期せぬ起動の防止	油空圧システムでは残圧による生ずるアクチュエータの起動など蓄積されたエネルギーによる起動と保全モード等の動力復帰後の予期しない起動の防止.
遮断及びエネルギー消散	動力遮断装置，蓄積エネルギーの消散または制限装置を示しZMS（Zero Mechanical State）[27] による安全確保策である.

表 2.4 は制御システムの安全関連部における安全確保の性能分類で，保護カテゴリと呼ばれている．同表で，要求事項は制御システムの保護方策（安全確保方策）として実施すべき事故を指し，安全機能の維持能力は実施の保護方策の限界を表している（制御システムに関するリスクアセスメント上での危険源を意味する.）同表中で不具合とは，制御システム内の部品故障の他に，機械的構造として，例えば嵌め合いの緩みなどを含む．また，不具合の蓄積とは，複数の部品がシステムを修復する前に故障するような，多重故障の発生を意味している．表 2.5 に表 2.4 に対応して実施されると考えられる技術的方法例を示す．同表で基本安全原則とは，制御システムとしての機能の信頼性確保は当然実施すべきことを意味する．

表 1 でカテゴリ B のシステムは，カテゴリ 1 から 4 で示される要求事項を含まず，単に目的機能を果たすだけの制御システムの場合である．カテゴリ 1 のシステムは主として機械的コンポーネントに対する要求事項で，安全上で十分に吟味された安全原則として，閂やカムなど剛性に基づく力の伝達構造が要請される．基本的には機械的構造の高信頼化に基づく．

カテゴリ 2 のシステムでは，安全確保の機能はある時間間隔でチェックされるべきことを要請する．カテゴリ 3 のシステムは，単一故障（不具合）における影響を回避する目的から，二重系が示してある．カテゴリ 4 のシステムでダイバーシティ（多様性）とは異種技術の適用を意味し，例えば機械的出力を，シーケンサと電磁リレーで制御するような方法である．このカテゴリはMTTFd（危険側故障発生確率），DCavg（診断サイクル），CCF（共通原因故障）により評価が行われる [28] ．

表 2.4 カテゴリごとの要求事項のまとめ

カテゴリ	要求のまとめ	システム動作	安全実現のための原則	各チャネルのMTTFd	DCavg	CCF
B	SRP/CS 及び/又はその保護装置は，その部品と同じく，予期される影響に耐えられるよう，関連規格に従い，設計，構築，選択，組み立られていること．基本の安全原則が使用される．	故障が発生すると安全機能の喪失を招くことがある．	主に部品の選択によって特徴づけられる．	低から中	なし	関連なし

表 2.4 続き

1	B の要求が適用される．十分検討された部品と安全原則が使用される．	故障発生率はカテゴリ B より低いが故障時は安全機能の喪失を招くことがある．	主に部品の選択によって特徴づけられる．	高	なし	関連なし
2	B の要求と十分検討された安全原則が適用される．	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．安全機能の喪失は点検により検出される．	主に部品の選択によって特徴づけられる．	低から高	低から中	
3	B の要求と十分検討された安全原則が適用される．安全関連部品は以下のように設計される． 一．単一故障が安全機能の喪失を招かないこと． 一．実行可能な限り単一故障は検出される．	単一故障発生時，安全機能は動作する．すべてではないが故障を検出できる．検出されない故障が累積した場合，安全機能の喪失を招くことがある．	主に構造によって特徴付けられる．	低から高	低から中	
4	B の要求と十分に検討された安全原則が適用される．安全関連部品は，次のように設計される． 一．単一故障が安全機能の喪失を招かないこと． 一．単一故障は，次の安全機能が働く前に検出されること．検出が不可能でも累積が安全機能の喪失を招かないこと	単一故障発生時，安全機能は動作する．累積故障の検知により安全機能の喪失率は減少する．（高い DC）安全機能喪失を防止するため，故障はすぐに検知される．	主に構造によって特徴付けられる．	高	高（累積の故障を含む）	

2.6　ISO13849-2（制御システムの安全関連部：妥当性確認）

ISO13849-2（制御システムの安全関連部：妥当性確認）では機械類の全体的な安全要求仕様内で, 制御システムの安全関連部の設計仕様及び適合性を確認することを目的としている．その中で付属書Bには空気圧システムにおける基本的安全原則，十分に吟味された安全原則および構成品, 不具合リストおよび不具合の除外について規定されている[(29)]．

2.6.1　空気圧システムの危険性と基本安全原則

基本安全原則とは, 安全に関わる制御システムにおいて意図する使用に対して適切な設計・製造であって，使用環境に対して信頼性を有するとともに，機械制御システムの安全性確保の基本原則として, 機械の起動は動力の供給に基づき停止はその遮断により, かつ，機械の停止時には予期しない起動の防止を有することと定義できる．表 2.5 に空気圧システムにおける基本安全原則の例を示す[(29)]．

流体技術を利用する空気圧システムで発生する可能性のある危険状態は, 次の事象または状態の発生が予測される.

（1）制御されない加圧流体の流出
（2）意図しない機械の動作
（3）許容されない操作出力
（4）有害な使用流体との接触

（1）については配管からの漏洩や配管破損による流体噴出が直接人体に危害を与えたり, 間接的には人の滑りの要因となったり, 引火の危険性を考えることができる. (2) については，仕様上（構造，制御機能，流体特性等）の誤り，システム要素の不具合などにより生じ得る．(3) には制御されない過圧力の出力を，(4) には人体への毒性の影響を考えることができる.

空気圧システムにおける上述のような危険源に対する保護方策として，表 3.2 の具体的な安全原則が示される．同表の安全原則項目は，空気圧システムにおいてともにほぼ共通する．また，リスクアセスメントに基づく機械の安全設計の実施時における妥当性確認ツールのための情報として活用できる.

表2.5　空気圧システムの基本安全原則

基本的安全原則	具体的方策例
適切な材料の使用と適切な製造	応力，耐久性，弾性，摩耗，腐食，温度，流体種類等に応じて選定する．
適切な設計値の確保	応力，歪み，疲労，表面粗さ，公差等を考慮して，大きさや形状を設定する．
要素／システムの正しい選定，配置，組立，据付	製造者の指定（仕様書，適正締付トルク等）を遵守したり，類似品の良好な工学慣例を適用する．
エネルギー分離の原則の適用	エネルギー開放により安全状態を得て，起動時にエネルギー供給する（閉回路原理）．ただし，流体圧力損失時に新たな危険源を生じる場合は適用しない．
圧力制限	リリーフ弁（安全弁），減圧弁により規定値以上の圧力上昇を制限する．
速度制限／低減	絞り（弁），速度（流量）制御弁等により，流体流量を制限してアクチュエータの速度を抑制する．
流体汚染の十分な回避	塵埃，水分等をフィルタによりろ過，あるいは分離する．
切り替え時間の正しい範囲	エネルギー供給の中断，変動，回復などの過渡状態に影響する管長，摩擦，注油，慣性等を考慮する．
環境条件に対する耐性	想定し得る外的環境（振動，温湿度，汚染等）下で機能する．
予期しない起動の防止	残圧等の蓄積エネルギーや電源復帰，異なるモードによる予期せぬ起動を考慮する．残圧排出の特別な装置を要する場合もある．
分離・単純化	安全関連部と非安全関連部との分離，及び要素数を低減する．
正しい温度範囲	全システムで考慮する．

2.6.2　実績のある安全原則の適用

欧州では，安全上すでに十分に使用実績のある技術を“十分に吟味された安全原則”として定めて，その適用を推奨する[24]，[30]以下にその例を示す．

（1）過大な諸元（安全率）
　十分余裕のある定格を設定する．

（2）安全位置
　要素の可動部停止の位置は機械的摩擦による手段だけでは不十分である．ロック機構，ばね等により安全側となる位置に固定され，位置変更には力を必要とする．表2.6の（4）および（6），（8）が対応する．

（3）オンにする力（駆動力）よりオフにする力（閉塞力）の方を大きくする．
　例えば，スプール形弁でのスプールの切換りにおける，操作力とばね復帰力の関係は，安全位置に動作させる力の方がオン側操作力により大きくとる．この場合の，OFF/ONの比は安全率と見なすことができる．

（4）負荷圧で閉じる弁
　一般的にはシート弁構造（ポペット形）がこれに該当する．

（5）十分に吟味されたばねの使用
　材料，製造手段，処理が念入りに行われ，十分にガイドされ，疲労に対する十分な安全率を持つばねとされる．表2.6の（5）および（6）が対応する．

（6）規定流量に対する抵抗による速度制限／低減
　固定のオリフィス（円状孔絞り）や固定のスロットル（絞り弁）により流量制御がこれに当る．

（7）力制限／低減
　十分に吟味されたばねを持ち，適切な大きさで適切に選定されたリリーフ弁で実現されている．見かけ上では，表2.6が対応する．

（8）機械的ポジティブ動作の原理
　要素の可動部が，ばねや摩擦ではなく剛性要素を介して接続され，作動力が伝達され動作するような機構をポジティブ動作と呼ぶ．表2.6の（6）のスプリング停止はこの原理に基づく．

（9）冗長部品
　ばねを複数組込む等，要素の冗長化によって要素の不具合の影響を低減する．

（10）スプール弁の十分なポジティブオーバーラップ
　スプールとスリーブのポートが重なりを持つものをオーバーラップと呼ぶ．これによりスプールの移動で漏れの発生を防止できる．これはアクチュエータの危険な動作を防止する構造を示しており，弁の安全機能上で重要な特性となる．

（11）制限されたヒステリシス

摩擦の増加や材料公差の組合せがヒステリシスに悪影響を及ぼす場合，適切な材料の選定や潤滑が必要である．

（12）流体汚染の適切な回避，状態監視

フィルタによる高度なろ過, および微粒子と水分の流体からの分離を考慮するとともに，ろ過状態の表示を考慮する必要がある．なお，空気圧の場合はドレンの排出を含む.

（13）動作条件の適切な範囲

動作条件の制限（圧力範囲，流量範囲，温度範囲）を考慮する．

2.6.3　空気圧コンポーネントレベルの安全原則例とその適用例

空気圧システムでは, アクチュエータがシステム外部へ機械的エネルギーを出力する部分であることから, アクチュエータの動作が障害発生時に安全側となるように特に配慮する必要がある．空気圧コンポーネントについての安全原則例とその適用例を表2.6に示す. 同表で基礎的安全原則とは, 国際規格ISO13849-2で言及される安全原則である．同表ではこの安全原則が可能と考えられる空気圧コンポーネントを示している．

表2.6　空気圧コンポーネントにおける安全原則とその適用例

基礎的安全原則例			適用のコンポーネント例
(1)	流路遮断による安全確保	流路を遮断して出力を制限する	全てのコンポーネント，特に可変絞り弁
(2)	流体飛散の防止	流路の強化／2重化する	管路，接続点
(3)	出力停止による安全確保	動力供給の停止による安全確保	油圧ポンプ，方向制御弁を除くすべて
(4)	スプリング施錠／動力駆動	スプリングで施錠状態とし，動力で解錠する	逆止め弁，押しボタン
(5)	スプリングの安全原則	ばねコイル径以下の空隙での圧縮ばねの使用	単動シリンダ，方向制御弁，空圧電磁弁，電磁比例圧力弁

表2.6続き

(6)	スプリング停止／動力駆動	スプリングによる制動／動力による制動解除	単動シリンダ，方向制御弁，空気圧電磁弁，電磁比例圧力弁
(7)	制御流駆動／自由流排出	駆動側は制御された流路とし，排出側は自由流とする	単動シリンダ，速度制御弁
(8)	調整機構のロック	調整機構をロックする．ロックの解錠を許可制とする	可変絞り弁
(9)	可動部固着の検出	可動部の移動を位置スイッチで確認する	単動シリンダ，方向制御弁，空気圧電磁弁，電磁比例圧力弁，逆止め弁

2.7　空気圧システム通則 ISO4414

空気圧システム通則ISO4414（Pneumatic fluid power-General rules relating to systems）[31]は工場棟の製造工程に用いられる空気圧システムについて規定されており安全，故障及び事故の無いシステムの運転，簡単で経済的な保守，システムの長寿命を適用範囲として構成されているタイプB規格である．

その中で安全についての要求事項は（1）～（7）について規定されている．

（1）設計上の考慮
（2）機器の選択
（3）予期しない圧力
（4）機械的な動作
（5）騒音
（6）漏れ
（7）噴流によって運ばれる有害物質

（1）～（7）では空気圧回路の設計で故障が発生した場合に人体の安全を最優先して，機器や環境の損傷を最小限にすることを規定している．そのため，機器の選択では機器の信頼性に注意して，危険側誤りによる危害の防止，圧縮空気の漏れによる危害などを防止することが求められおり，空気圧コンポーネントのストレス・ストレングス・モデルによる強度設計，システムのガードなどによる防護，リリーフ弁などによる減圧によって安全を構成することを求めている．

2.8　空気圧コンポーネントおよび制御装置の特別要求事項

欧州規格EN983 では空気圧システムにおけるコンポーネントおよび制御装置に関する特別要求事項を詳細に述べている [30]．表 2.7 にその概略をまとめて示す.

表 2.7　空気圧システムのコンポーネントおよび制御装置に関する特別要求事項

要求事項
(1) モータおよび回転アクチュエータ 回転軸とその連結は防護すること.
(2) シリンダ ピストン棒の座屈耐性．衝撃耐性，振動耐圧を持つこと．上下視点のロック装置要．非意図的横荷重のない配置．全力耐性の取付締付具とする. シリンダの通気要．ピストン棒の損傷防護要.
(3) 弁 正確な機能と適切な気密性要．取付け方向誤り防止付き．主要素の重力・衝撃・振動配慮の取付け．故障時の非対称性を配慮すること．機械作動弁は作動装置から損傷を受けないこと.
(4) 電気操作弁 電気接続はIEC60204-1による．ハウジングはIEC60529による防護要．ソレノイドは公称電圧の±10%で開閉できること．マニュアル・オーバライド（手動切替）機構を備えること.
(5) エネルギー伝達 圧縮空気／中性ガスの有害物質除去の手段を講ずること．フィルタの効果を示す手段をもつこと．潤滑油の適合性を配慮のこと．配管は足場や梯子として利用可能なこと．異物の侵入を防止すること．継手の取付け／取外し危険があるときは，制御圧開放装置を備えること．ホースは最小曲げ半径以上のこと．ユニバール・リットルを超える円形容器は遮蔽すること.

表2.7続き

（6）システムの防護 圧力を安全限度内に維持するための制御装置を備えること．圧力・流量の不正変更が危険源を引起すときは，不正行為防止装置を備えること．設備が連動自動／手動の制御を備えており，いずれかの故障が危険源となる場合，防護インタロックその他の安全手段を設けること．アクチュエータに過大外部荷重がかかる場合，防護手段を講じること．アクチュエータの予期しない危険作動を防止する機能を備えること．等

2.9 安全システム

2.9.1 安全システム全般

安全システムはシステムの入力と出力の関係が単調な論理関係で構築されることを理想としている[32]．したがって一般的に機械コンポーネントはポジティブな機械的結合でエネルギーを伝達することが安全原則として要求される．しかし，油圧・空気圧システムはポジティブな機械的結合によるのでなく，流体の圧力によりエネルギーが伝達される構造である．その場合，コンポーネントにおける流体の圧力によって動作するばね（スプリング）の働きによって単調な論理関係を実現するが，そのばねの動作に対して十分な配慮が必要である．

2.9.2 安全（確認）の原理

安全には杉本，蓬原，向殿によって「安全（確認）の原理[33]」が提案されている．安全（確認）の原理とは“危険を伴う機械的操作は，安全の確認を許可の条件とする”という基本的考えが与えられる．安全（確認）の原理は，安全を維持する操作に危険側誤りが含まれる場合，安全を常時確認し，安全が確認できないときはシステムを停止するインタロックの必要性を主張する．ここでのインタロックとは危険源である動力供給を遮断して運転を停止させる「決定論」であることを証明することであり，本研究では安全（確認）の原理は動力遮断であることを主張する．

安全（確認）の原理では「安全」は先に危険が認識され，それを予測して回避する過程で生ずる概念である．機械が出力を生ずるとき，事故が予測されるとき（危険のとき）機械的出力を停止することによって事故を防ぐことができる．しかし，この危険状態には，本来「危険」と「安全」の何れかであるが，「危険，安全のどちらでとも言えない（不安）」が存在する．すなわち，不安を危険に含むことにより事故を確実に防止することが可能であると言える．したがって，不安を論理変数A（t）∈｛1，0｝で表し，不

安なときを 1，不安でないときを 0 とし，この不安を含む危険状態を論理変数H_C（t）∈｛1，0｝で表せば（2.5）式が成立する．

$$H_C(t) = A(t) \vee H(t) \tag{2.5}$$

ここに，記号∨は論理和で，H（t）∈｛1，0｝は明らかに危険な状態であることを意味している．真の危険H（t）の否定￢H（t）を安全とし，￢H_C（t）を予想される安全とすれば，（2.5）式によって次の論理的関係が成立しなければならない．

$$\neg H(t) \geqq \neg H_C(t) \tag{2.6}$$

（2.6）式は，安全でないのに￢H_C（t）＝1として安全が予測されてはならないことを示しており，安全（確認）の原理を表している．

2.9.3　安全確認型システムと危険検出型システム

図 2. 15（a）に示す危険検出型システム [34] は，危険な状況を検出し，その信号によってそこに人を立ち入れないようにしたり，機械を動かさないようにしたりするシステムのことである．例えば，踏切の信号機や遮断機は，危険検出型である．列車が近づいて危険な状態になると，それを音と光で知らせ，遮断機を下ろして人が立ち入らないようにするのである．このようなシステムは，一見すると安全を確保しているように思えるかもしれない．しかし機械も制御装置も故障する可能性があり，故障は検出装置にも起こる．危険検出型の場合，その検出装置が故障すると，危険が無いものとして扱われることになる．たまたま通行者が電車の接近に気づき回避できれば幸いだが，気づかなければ事故になる．

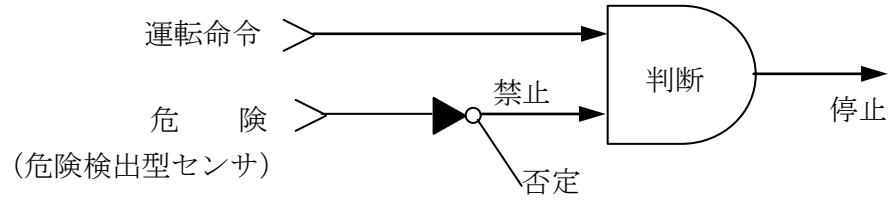
つまり，危険検出型システムでは，利用者の安全は検出装置が故障していないかどうかの「賭け」の上に成り立つ安全になっている．機械は多くの人々に多くの回数使用されるのであるから，「賭け」の安全しか実現していない危険検出型システムでは，どこかで必ず事故が発生するのである．

現状の空気圧システム（図 2.6）では安全システムのリリーフ機能（リリーフ弁，安全弁，ラプチャーディス等）が故障しても高圧空気が供給され続けるため危険検出型と見ることができる．危険検出型システムはセンサで危険が検出できれば停止することが可能であるが，センサが故障して機能喪失した場合に運転を継続してしまう「賭け」の安全しか実現しないシステムであると言える．

徹底して「賭け」を回避するには，危険を検出するのではなく，安全を確認するシステムにすればよい．安全を検出し，安全を検出できなくなったとき，危険と判断して止めるのである．

信号に例えると，危険検出型システムは「赤」を点灯して運転を停止させる．故障で「赤」を点灯できないと事故になってしまう．それに対して安全確認型システム[34),(35)]では，安全を「青」の点灯で知らせ運転を許可する．故障で，安全を「青」の点灯で通報できないと機械は止まり，安全が確保される（図 2.15（b））．

もともと安全装置はフェールセーフに設計し，壊れる場合には必ず安全側故障となり，安全信号を発信しないようにする必要がある．安全確認型の安全装置は，そのままフェールセーフになる（例：表 2.8（a），図 2.15（b））．あるいは，壊れて困る部品は，多重化するなどして異常動作を自己診断でき，正常動作の確保や安全の確認ができるようにする．重要なことは，安全の確認をオン信号で知らせ，故障で安全が確認できないときは停止をオフ信号で知らせることである．

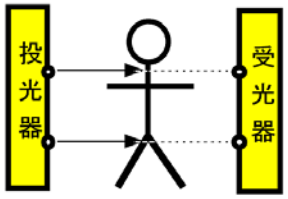
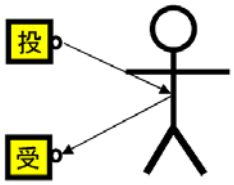
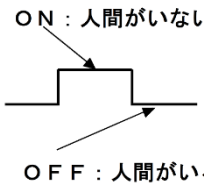
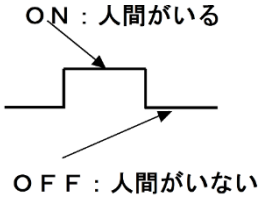


（a）危険検出型インタロック

（b）安全確認型インタロック

図2.15　安全確認型システムと危険検出型システム[34)]

表2.8　光線式センサの故障モード

	安全確認型	危険検出型
	（a）透過型	（b）反射型
装置の形態		
受光器出力		
故障時	受光器出力OFF （安全側故障）	受光器出力OFF （危険側故障）

安全確認型インタロックを空気圧システムに導入した場合には動力遮断および排気によりリスクの解消を行うことが可能である．したがって，現状の空気圧システムの安全は許容リスクレベルの達成でリスクに逃げており，動力遮断によりリスクを解消するまで追及していないことが明らかであることがわかる．

安全確認型の例としてガス湯沸かし器（図 2.16）[36] を示す．安全確認型のインタロックシステムの例で，バーナに炎が存在するときのみガスが供給されて燃焼を維持できる点火装置である．ツマミを押すと点火装置を起動してバーナが着火される．着火後は熱電対で炎の存在が検出され，熱電対電流が電磁弁の電磁石に流れて接極子を吸引し，ガス流路の弁を開き続ける．炎が存在しなくなると熱電対電流が発生しないので，電磁石の吸引力が失われて，弁は閉じてガスの供給が遮断される．すなわち，図 2.16 のこの機器を構成する①～④の何れに故障が生じてもガスの供給が遮断されるシステムである．

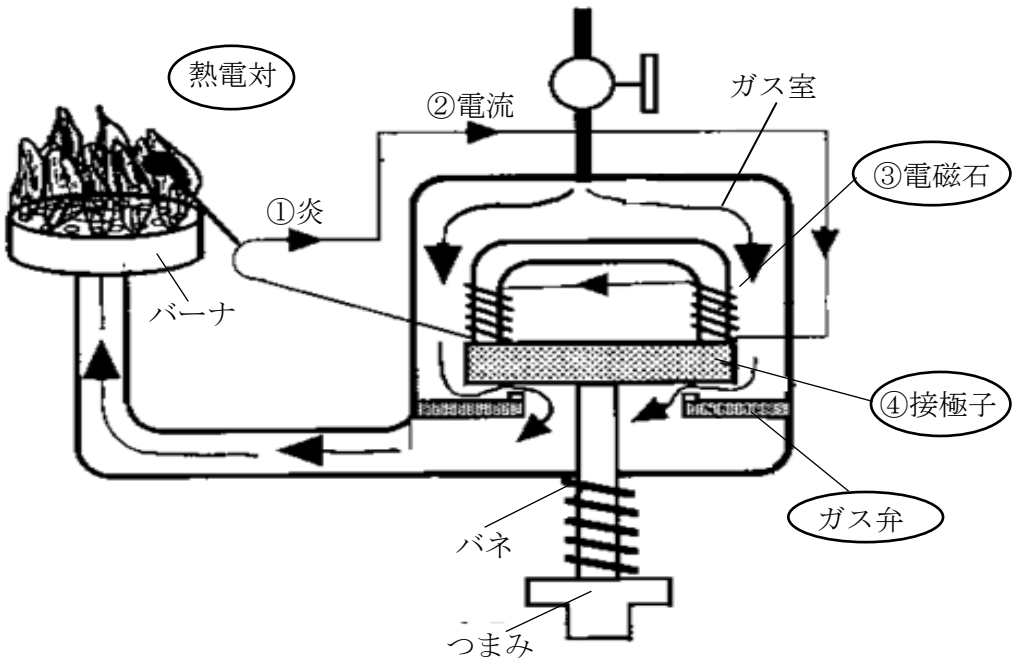


図2.16　安全確認型インタロックシステム例（ガス湯沸かし器）

2.9.4　安全確認システムを実現するインタロックシステムの条件

インタロックシステムを構成する際に（1）～（4）の条件を満たすことによって安全確認システムであるインタロックシステムを実現することが可能である.

（1）設計者によって示される安全の条件には誤りが許されない.

（2）安全の確認とは，安全の条件を維持する操作の正常性の確認を意味し，危険を伴う機械的操作は，安全確認を許可の条件とする.

（3）故障で安全が確認できないときは「危険」と見なして機械的操作を停止（動力遮断）する.

（4）停止には危険側誤りが許されない.「停止」は動力源遮断を伴い，停止機能の危険側故障の影響を抑制する.

2.10　小括

本章では，本研究を行うのに必要である空気圧システムの機能，概念および基本構造を述べ，一緒に各種コンポーネントの機能，図記号による表現と動作プロセスについて説明している．空気圧 システムでは動力である圧縮空気が配管を経由して制御部でその圧力，方向，流量を外部から別の電気的エネルギーまたは手動弁すなわち信号のエネルギーで制御されて出力され，アクチュエータで仕事をする構成になっている．

このプロセスの中で空気圧システムにおける事故（危害）について考察するとアクチュエータとの衝突や挟まれなどの事故（危害）と制御による危険側誤りによるコンポーネントの損傷や破裂，圧縮空気の噴出などによる事故（危害）の可能性が考えられる．

そのため，国際安全規格ではリスクベースの考え方により，空気圧システムに関係する国際安全規格（2.4～2.8項に示す）では，空気圧コンポーネントの信頼性（強度的および機能的）と空気圧コンポーネントを設計する際のストレス・ストレングス・モデルによる設計，システム自体の防護，アクチュエータの危険動作の防止で安全を構成するように規定していると見ることができる．しかし，制御による危険側誤りの防止に関する規格の要求は見られない．そのため，空気圧システムで発生する可能性のある危険側誤りによる危険側故障について制御の段階で防止する安全の構築は見られない．

現状の空気圧システムの圧力制御に関する安全はリリーフ機能による排気のみで構成されており，リリーフ機能の危険側故障が生じた場合は高圧空気が出力されてしまう．

これは危険検出型の問題点であるセンサなどの故障が生じた場合に出力または運転が継続されてしまうことと同様である．

したがって，現状の空気圧システムの圧力制御に関する安全は危険検出型の特性であり動力遮断構造が存在しないため安全システムとしては不足していると言える．

ISO13849-1では制御システムの安全関連部についてはリスクベースであるため，カテゴリによる危険側故障発生確率による確率による評価であり，安全機能については停止に関する厳格な条件（例えば，事故の手前で停止するなど）は示されていない．

すなわち，現状では制御システムの安全関連部もリスク低減の方法の1つとされているため，危険側故障発生確率を低減すれば安全と見なされており完全に許容不可能なリスクへの対応がなされているとは言うことはできない問題点があると言える．

したがって，リスクベース安全（リスク低減）では安全を証明する概念がない，安全（確認）の原理では安全の証明は止まること（動力遮断（リスク解消））である．

第 2 章　参考文献

(1) 山元智成，池田博康，蓬原弘一，油空圧安全コンポーネントにおける危険源分析と安全原則の考察，信頼性学会第 17 回秋季シンポジュウム報文集， pp79-82（2004.11.19）

(2) 大津亘著，“中小企業に役立つ FMEA 実践ガイド”，日本規格協会，pp.48

(3) 中村瑞穂，蓬原弘一，空気圧制御システムの論理構造とその適用，信頼性学会第 19 回秋季シンポジュウム報文集，pp73-76，（2006.10.20）

(4) “空気圧技術初級テキスト　2.空気圧機器　2.1 空気源と清浄化システム”，SMC 株式会社，pp.1，1995，初版（印刷）

(5) 空気圧技術初級テキスト“2.空気圧機器　2.1 空気源と清浄化システム”，SMC 株式会社，pp.9，1995，初版（印刷）

(6) 雇用・能力開発機構　職業能力開発総合大学校　能力開発研究センター編，“空気圧シーケンス制御　シリーズ 1（機器編）”, 社団法人　雇用問題研究会, pp178, 2002，改定第 1 版

(7) （社）日本油空圧学会編　“油空圧便覧”，株式会社オーム社，pp.509，1989，第 1 版

(8) 中西康二　著，“基礎から学ぶ空気圧技術”，オーム社，pp.34，2001，第 1 版

(9) 仙田良二　著，“実践メカトロニクス　油圧・空気圧”，産業図書，pp7，2000，第 10 版

(10) 空気圧技術初級テキスト“2.空気圧機器　2.4 圧力制御弁”, SMC 株式会社, pp.9, 1995，初版（印刷）

(11) 空気圧技術初級テキスト“2.空気圧機器　2.5 ルブリケータ”，SMC 株式会社，pp.18，1995，初版（印刷）

(12) 笹川宏之，古井英則，中村瑞穂　著，“PLC によるメカトロ制御入門”，日刊工業新聞社，pp156，2011，初版

(13) 空気圧技術初級テキスト“2.空気圧機器　2.9 速度制御弁”, SMC 株式会社, pp.35, 1995，初版（印刷）

(14) 空気圧技術初級テキスト“2.空気圧機器　2.8 アクチュエータ”，SMC 株式会社，pp.1，1995，初版（印刷）

(15) 日本プラントメンテナンス協会編，入門・機械＆保全ブックス 油・空圧の本②，第 5 版(2003)，pp.179，日本プラントメンテナンス協会.

(16) 笹川宏之，古井英則，中村瑞穂　著，“PLC によるメカトロ制御入門”，日刊工業新聞社，pp148，2011，初版

（17）ISO/IEC Guide51:1999 Safety aspects – Guidelines for their inclusion in standards,（1999）, International Organization for Standardization.
（18）向殿政男，宮崎浩一　著,“安全の国際規格　第 1 巻　安全設計の基本概念”，第 1 版，2007，pp.23，財団法人　日本規格協会
（19）向殿政男，宮崎浩一　著,“安全の国際規格　第 1 巻　安全設計の基本概念”，第 1 版，2007，pp.31，財団法人　日本規格協会
（20）蓬原弘一　監修,“基本安全規格に基づく安全構築技術 – JIS B 9700:2004-”，初版（2006），pp.57-58，安全応用研究会
（21）ISO12100-1:2003,Safety of machinery-Basic concepts and general principles for design, Part 1 : Basic terminology , methodology(2003) , International Organization for Standardization.
（22）ISO12100-2 : 2003, Safety of machinery-Basic concepts and general principles for design, Part 2：Technical principles(2003), International Organization for Standardization.
（23）蓬原弘一，田中紘一，鈴木正俊　編著,“生産現場に役立つ安全技術 -リスクアセスメント実践で知っておきたい安全技術-”，初版（2010），pp.21，安全応用研究会
（24）ISO13849-1:2006，Safety of machinery-Safety-related parts of control systems，Part1:General principles for design(2006) , International Organization for Standardization.
（25）ISO14121:1999, Safety of machinery-Principles of risk assessment,（1999）, International Organization for Standardization.
（26）向殿政男, 宮崎浩一　著,“安全の国際規格　第 2 巻　機械安全”, 第 1 版, 2007, pp.43，財団法人　日本規格協会
（27）OSHA29 CFR 1910.147,The control of hazardous energy（lockout/tag out）, U.S.Department of Labor Occupational Safety & Health Administration.
（28）蓬原弘一,“2 値論理値を用いて安全原則を考える”,日本信頼性学会誌，Vol.29, No.2(2007)，pp.80-90.
（29）ISO13849-2:2003，Safety of machinery-Safety-related parts of control systems-Part 2:Validation(2003)，International Organization for Standardization.
（30）EN983 Safety of machinery-Safety-requirements for fluid power system and their components-pneumatic.
（31） ISO4414:1998，Pneumatic fluid power-General rules and safety requirements for systems and their components(1998)，International Organization for Standardization.

（32）蓬原弘一著，“安全基礎工学 –安全構築の基礎-”，初版（2004），pp.13-15，安全応用研究会
（33）杉本旭, 蓬原弘一,“安全の原理”,日本機械学会論文集 C 編, Vol.56, No.530(1990), pp.75-83.
（34）（社）実践教育訓練研究協会　編，“安全管理技術”，初版（1999），pp.63，工業調査会
（35）杉本旭，蓬原弘一，向殿政男，“安全作業システムの原理とその論理的構造”，電気学会論文集 D 編，Vol.107D，No.9(1987)，pp.1092-1098.
（36）安全技術応用研究会　編著，“国際規格対応　安全システム構築総覧「機械／電気安全」「機能安全」“，初版（1999），pp.91-92，株式会社通産資料調査会.

第 3 章　空気圧システムの故障解析

3.1　はじめに

本章では，図 2.3 の空気圧システムの代表的構成例を構成している，各種コンポーネント（13 種類）について FMEA（Failure Mode and Effects Analysis）を実施して故障時の挙動について分析を行った．その結果，システム内部の圧力が上昇する側，低下する側の両側に危険側故障の原因となる故障モードが存在することが分かった．また，分析した結果について BIA-Report6/97e と ISO13849-2 の付属書 B（空気圧システムの妥当性確認ツール）との比較を行い故障モードの偏り等について検討を行い本質的な違いが無いことを示している．したがって，現状のシステムでは圧力上昇側の誤り（危険側誤り）を生ずるコンポーネントの存在を示すとともに，空気圧システムにおける故障監視には，圧力の上昇（危険側誤り）と低下の両方を検出する必要性があることを示している．

本章の構成は，第 3.2 節では FMEA の手法の説明，ワークシート，FMEA を実施するための分析レベル，影響度分析の範囲と実施手順を示した．第 3.3 節で分析結果を示しシステム内部の圧力上昇側と低下側の両側に危険側故障の原因となる可能性がある故障モードを明らかにし，圧力の上昇および低下側の両側の故障モードを監視対象とする必要性があることを示した．

第 3.4 節では第 3.3 節の FMEA の結果と BIA-Report6/97e，第 3.5 節では ISO13849-2 の付属書 B（空気圧システムの妥当性確認ツール）との比較を行い故障モードの偏り等について検討を行い本質的な違いが無いことを示した第 3.6 節では安全性確保上からの FMEA の限界について示した．

3.2　空気圧システムの FMEA

3.2.1　FMEA（Failure Mode and Effects Analysis）

FMEA（故障モード影響分析）はシステムにおけるすべてのコンポーネントの故障モードとその影響（制御システムの安全関連部の出力への影響）を審査する方法である[(1)]．

この分析は個々のコンポーネントの故障から出発し，それによって生じうる危険源を特定する．すなわち，この方法により制御システム内で採用される具体的保護方策の効果を審査することができる．

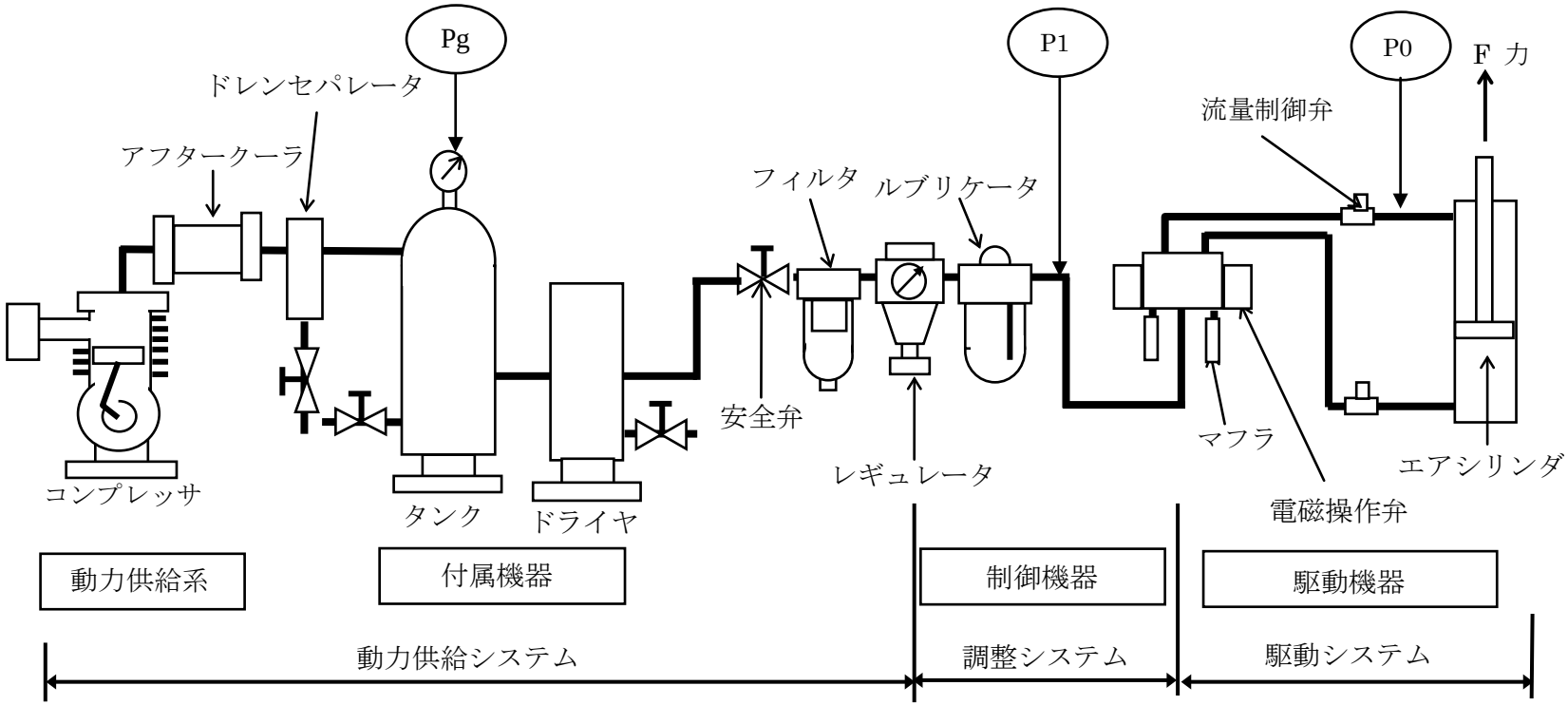


図 3.1　空気圧システムの構成例 [16]

3.2.2 FMEAの目的

図 3.1 の空気圧システムを構成する各種コンポーネントについて表 3.1 のワークシートでFMEAによる故障分析を実施する．FMEAによる抽出された故障モードが動力調整部出力P1（方向制御弁入口圧力），または，アクチュエータの駆動系圧力（P0）への影響の仕方について分析を行う．ワークシートにおける論理値はP1，P0 で出力するを 1，出力しないを 0 と示し，φについては危険側故障の可能性を意味する．すなわち，故障モードの発生が原因となる危険側故障の抽出を目的としている．

表 3.1 空気圧駆動システムのFMEAワークシート [2]

コンポーネント	故障モード	論理値	挙動 （方向制御弁入力P1またはシリンダ出力P0への影響）

3.2.3 FMEA の実施手順

FMEA の表形式の例としてワークシートを表 3.2 に示す. 図 3.2 に FMEA による分析手順を示す．同図における作業は以下の①～⑥の手順に沿って行われる．

表 3.2　基本的FMEAワークシート [3]

システム＿＿＿＿＿＿

機器名	機能	故障モード	原因	発生頻度	影響			検出法	致命度	RPN	対策	対策順位
					サブシステム	システム	安全性					

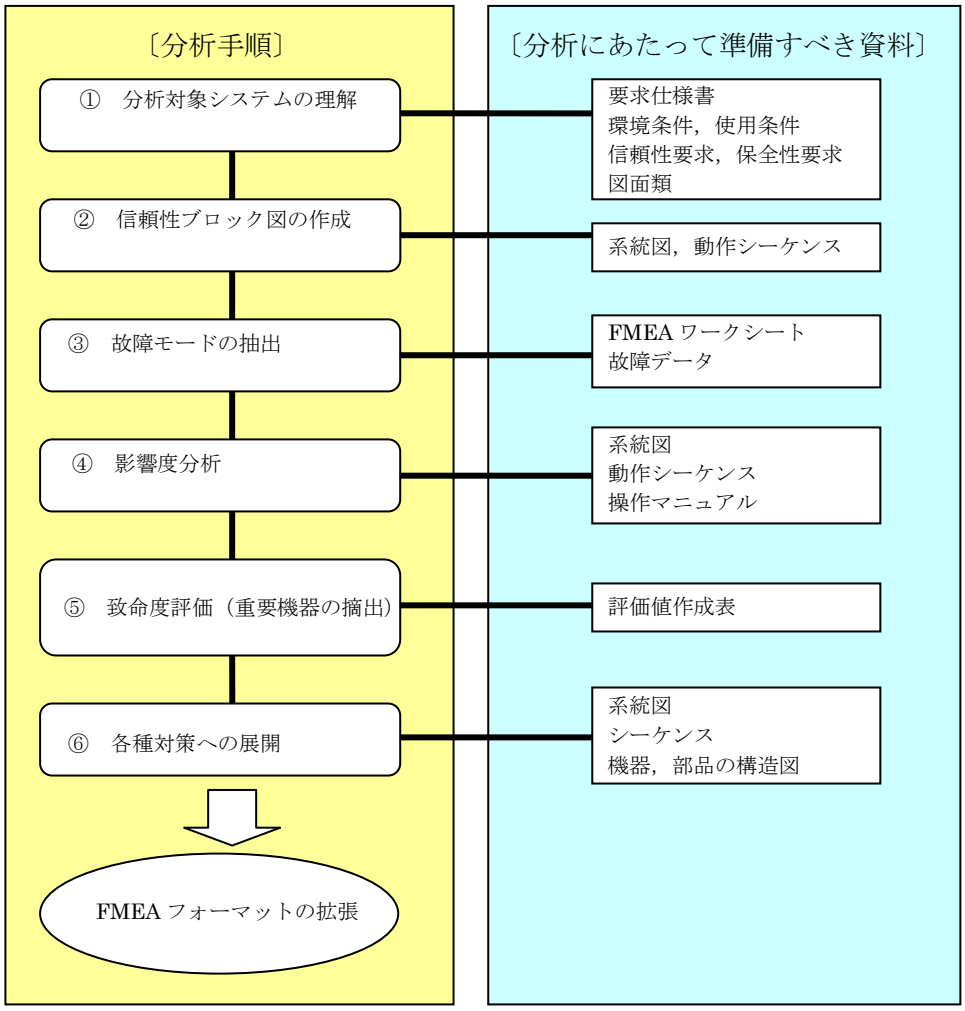


図 3.2　FMEA手順 [4]

①　分析対象システムの理解

分析対象のシステムの理解が分析の質を左右する重要な項目の一つであり，③で行う故障モードの摘出において最も重要な事項である．具体的に分析対象システムを理解するには，分析対象の製品の機能，性能，システムとしての任務，使用環境，起動・停止，運転条件（運転頻度，稼働時間等）を理解していることが必要である．

図 3.2 で要求仕様書とは，例えば製品の性能，経済性，信頼性，安全性，保全性などについて顧客から製造元へ要求するものである．信頼性要求とは，例えば製品のアベイラビリティ（稼働率），製品の設計寿命，定期的保全に伴う停止時間，故障率などについて顧客から製造元へ要求するものである．保全性要求は例えば製品の定期保全，故障診断，保全性プログラム計画，保全性作業の期間などについて顧客から製造元へ要求するものである．

② 信頼性ブロック図の作成

信頼性ブロック図はシステムの信頼度とそのコンポーネントとの間の運動伝達, 相互固定, 動力供給など機能的関連を示す線図である. 種類としては直列系と並列系の 2 種類がある. FMEAを行う上での信頼性ブロック図はシステム, サブシステム, ユニット, 使用機器（部品, 機器, 回路, モジュール等）部品などの分解レベルを表し, すなわちサブシステムや機器などの要素間の機能的な相互依存性を明らかにすることができる. 例えば図 3.3 の直列系または図 3.4 の並列系（冗長系）に分解することができ, 機能的な故障の追跡に利用できる. また, 図 3.3, 3.4 で示すR_1とR_2はそれぞれの故障の発生確率を示す.

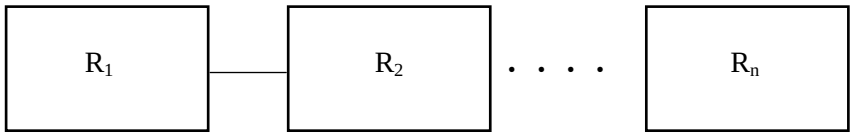


図 3.3　信頼性ブロック図（直列系）[5]

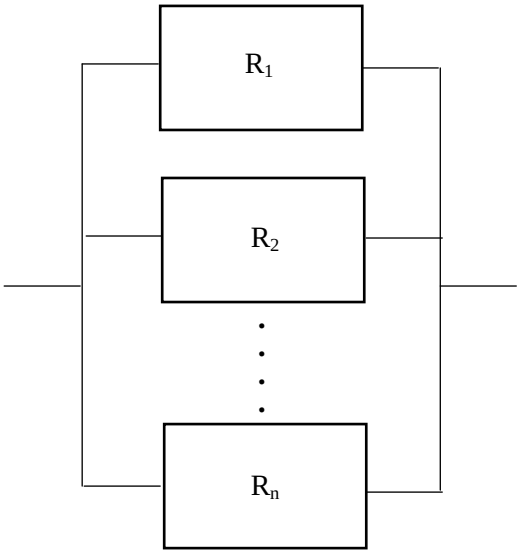


図 3.4　信頼性ブロック図（並列系）[5]

③ 故障モードの抽出

故障（Failure）とは国際規格では，「要求される機能を遂行する能力がアイテムになくなること」と定義される．また，障害（Fault）は「予防保全若しくは計画的行動又は外部資源の不足により機能を実行できない状態を除き，要求される機能を実行できないアイテムの状態と定義される」.

故障とはシステム，設備，部品が規定された機能（任務）を失う事である．故障の種類としては，機能停止型故障と機能低下型故障の 2 種類がある.

機能停止型故障は，システムや設備の全機能が停止するタイプの故障であり，原因は部分的な機能停止であっても，結果的にシステムの設備の全機能が停止するものである.

機能低下型故障は，システムや設備の部分的な機能の低下によって，全機能の停止には至らないが，いろいろな損失（不良，歩留り低下，速度低下，空転，チョコ停）を発生させるものである．故障モードは機器や部品で発生する故障（機能停止型故障，機能低下型故障）の状態であり，故障の現象である．それらの故障モードの例を表 3.3 に示す. 故障モードの抽出では，分析対象システムが運用されているときに発生する物理的，化学的，機械的，電気的，人為的な原因など，アイテム（システム，機器，部品など）が故障を起こす仕組み(故障のメカニズム)を考察することが必要となる.

表 3.3　故障モードの例 [6]

〔機能上の故障モード〕
動作しない，停止しない，早く作動，遅く作動，早く停止，遅く停止，時間的に不安定に作動，間欠的に作動，大きすぎる値，小さすぎる値，定位置に止まらない，定められた値にならない，誤動作，不注意な操作など.
〔機械系故障モード〕
摩耗，腐食，変形，亀裂，破損，脱落，焼損，漏れ，曲がり，固着，変色，異音，振動，共振，動作不良，ゆるみ，かじり，ずれ，傷，機械的加熱，機械的性能寿命など.

④ 影響度分析

影響度の分析は，図 3.2，表 3.2 に示すように，故障モードの発生によりサブシステムへの影響，システムへの影響，安全性，経済性など，どのような影響が生じるか，それを求める作業である．その作業では，分析レベルと影響度分析の範囲（レベル）をほぼ一致させる必要がある.

影響度分析の範囲（レベル）は，組織又は企業で設計改善又は工程・作業改善をできるレベルであることが基本であり，分析する前に図 3.5 に示すように分析レベルと影響度分析の範囲については明らかにしておくべきである.

この作業では，システムを構成するサブシステムおよび各種コンポーネントとの相関関係を信頼性ブロック図により用いて表し，故障の影響の及ぶ範囲を検討する.

表 3.2 の影響欄の各評価項目（サブシステム，システム，安全性等）に潜在している故障モードが発生した場合の影響の内容を記入して行く．表 3.2 のワークシートにはサ

ブシステム，システム，安全性のみの影響度分析であるが分析対象（製品）によっては社会的影響や環境への影響を引起す場合もあるので，その場合ワークシートを拡張して影響評価項目を増やす必要がある．

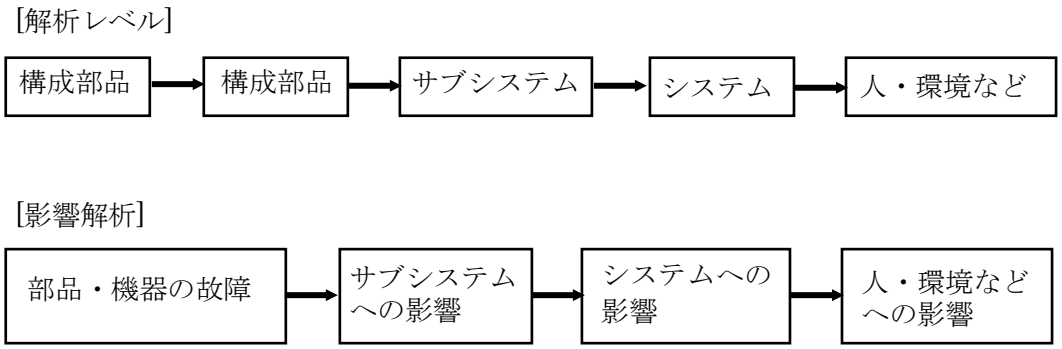


図 3.5　FMEAにおける分析レベルと構成部品の故障の影響分析のモデル図 [7]

表 3.4　影響度に対する評価レベルの設定例 [8]

評価レベル	評価基準	評価基準の具体例		
		システムへの影響	人への影響	車両の影響度
10	致命的	・システムに重大な損傷 ・システムに 2 つ以上の重大な影響を与える.	死傷，重傷	人身, 火災のような保安上の事故
8	重大 機能喪失	システムの一部に損傷	中程度のケガ	恐怖心が起きる事故
6	機能低下	システムに 1 つの重大な影響を与える	軽症	不快, 不安を感じる故障
4	軽微	・損傷は軽微 ・システムに与える影響はあまり大きくない	なし	少し気になる故障
2	極小	損傷は無視できる	―	気が付かない故障

表 3.4 に影響度分析の例を示す．各影響評価項目について認定される評価レベルによりレベル付け決定し，影響の程度（影響度）は次式に基づいて各影響項目の点数の和として求めることができる．

［影響度］＝［サブシステム］＋［システムへ］＋［安全性］　　(3.1)

影響度の項目については相対的重み付けをする目的で相対係数を乗ずることができる．例えば，ある製品が安全性および環境への影響を重要視する場合，その影響評価項目に各々5 倍および 2 倍の相対差を付けた場合，式（3.1）は式（3.2）で示すように影響度を算定する．ただし，各影響評価項目の評価レベルについては最高値を同じとする．

［影響度］＝［システム］＋［安全性×5］＋［環境　×2］　　(3.2)

⑤　致命度評価

致命度の評価は故障モードの発生頻度を表 3.5 の評価レベルとして求め，次の式（3.3）に基づいて影響度との積で求められる．

［致命度］＝［故障モードの発生頻度（評価レベル）］×［影響度］　　(3.3)

表 3.5　故障モード発生頻度の評価レベルの設定例 [9]

評価レベル	評価基準	評価基準具体例		
		発生頻度	故障回数 （λ;10E-3）	工程内 発生確率
10	発生頻度が非常に高い	1 回/週以内	8 回以上 （3.20）	1%以上
8	発生頻度が高い	1 回/月以内	5 回～8 回 （1.60～3.19）	0.1～1.0%
6	故障の可能性がある	1 回/年以内	3 回～4 回 （0. 80～1.59）	0.01～0.1%
4	少ないが起こりうる	1 回/5 年以内	2 回 （0.40～0.79）	0.001～0.01%
2	故障はほとんど起こらない	1 回/5 年以上	1 回以下 （0.39）	0.001%以下

危険優先数（RPN:Risk Priority Number）を次の致命度評価では「故障モードの発生頻度」と「影響度」の評価に加えて障害の検出方法を評価するために式（3.4）で定義する．この危険優先数による評価は，品質管理上からの製造，検査段階の FMEA で使われる場合が多い．

$$[危険優先数]=[故障モードの発生頻度]\times[影響度]\times[検出度] \quad (3.4)$$

FMEA 作業で分析される各種障害はできる限り，それが検出されなければならない．検出は例えば，製品が市場へ投入された時点，出荷時，製造時など故障モードが検出された段階を示す．分析と検出の関係は式（3.4）のように RPN の評価で故障モードが発生した段階について評価を行う．

検出方法については，故障モード，故障原因のいずれかを分析するかを検討して，検出器の検出精度，大きさ，重量，環境適合性，寿命などを検討して重要故障モードを見逃さないシステムの構築が必要とされる．

⑥　各種対策への展開

抽出された故障モードは，製品・システムの弱点であることから，重要性の高い順に対策を施す必要がある．重要な点は, FMEA の結果が設計改善または運用工程改善に反映されることである．例えば自動車業界のセクター規格である TS/ISO16949:2002 における設計・工程の両 FMEA では，推奨処置，対策時期，対策部署，担当者を決め，実行された対策について再度，影響度分析，RPN（危険優先度）を要請する．

3.3　空気圧システムにおけるFMEA分析結果と考察 (2)

FMEA分析における結果の一部を表3.6に示す．表3.6の故障モードは，動力調整部出力P1（方向制御弁入口圧力），または，アクチュエータの駆動系圧力（P0）への影響の仕方で表している．一部を示すことで限界だが，13のコンポーネントにおける故障モードは220件に上り，そのうち，15件（6.8%）はシステム内部の圧力（P1又はP0）が上昇する側の故障モードで，140件（64%）はシステム内部の圧力が低下する側の故障モードであった．また，残りの65件（30%）は圧力の変化に影響しない故障モードである．

図3.1の空気圧システムにおける圧力調整は，設定された圧力を超えようとするとき，レギュレータによって空気をシステム外部へ開放して圧力上昇を抑えるという方法で実行される．

レギュレータは，破裂の原因となる異常な圧力上昇を防ぐ機能を持つが，一般に，バネを用いるリリーフ機構は危険側の故障（圧力が上昇又は圧力が低下できない側の故障）を生じうるにも拘らず，安全弁，リリーフ弁，減圧弁などを併用する方法に止まり，故障の監視は殆ど行っていない．また，当然，圧力が低下する側の故障は安全側の故障として監視の対象から外されてきた．

残留リスクとも関係するが，一般に，危険側故障（誤り）の可能性がある場合それを防ぐために監視を必要とするが，レギュレータによって圧力調整を行う場合，FMEAの結果から，圧力が上昇する側と低下する側の両方の故障モードを監視対象とする必要がある．なお，圧力P0によるアクチュエータ出力は，人間との接触危険性に関わるが，ここでは，圧力の調整の誤りに関わる安全に限定して検討する．

表3.6　空気圧制御システムに対するFMEAの結果の例

コンポーネント	故障モード	論理値	挙動（方向制御弁入力P1，シリンダ出力P0への影響）
コンプレッサ	電源停止	0	コンプレッサが動作しないため，圧縮空気が供給されないので入力P1発生せず．
	モータ故障		
アフタークーラ	容器の一部破損	0	破損箇所より，圧縮空気が漏れるので入力P1 発生せず．
ドレンセパレータ	ボウル部破損	0	破損箇所から圧縮空気が排出され，入力 P1 が発生せず．
タンク	本体破損	0	破損箇所より，圧縮空気が漏れるので入力P1 発生せず．
ドライヤ	冷却器破損	0	破損箇所から圧縮空気が排出され，入力 P1 が発生せず．
安全弁	操作部のはずれ	0	弁体が閉じた状態では，圧縮空気が流れず，入力 P1 は発生せず．
		1	弁体が開いた状態で，圧縮空気が排出されており入力P1が発生する．
フィルタ	フィルタエレメント目詰まり	0	フィルタエレメントが90%以上塵埃などで，目詰まりしたら入力P1は発生せず．

（表 3.6　続き）

レギュレータ	調整バネ折損	0	ハンドルを回しても圧力調整ができず, 設定圧力値が0MPaであれば，主弁が閉じているので圧縮空気は通過できないので入力P1は発生せず.
		1	ハンドルを回しても圧力調整ができず, 空気圧制御システムで必要な設定圧力値であれば入力P1は発生し続ける.
		ϕ	ハンドルを回しても圧力調整ができず, 設定圧力値が低い値であれば，入力P1は発生する.
ルブリケータ	ボウル破損	ϕ	破損箇所から潤滑油が漏れ, 圧縮空気漏れによる圧力低下が発生する.
マフラ	ごみ詰まり	0	シリンダ前側から排気される圧縮空気が排気ポートからマフラを通るときごみ詰まりにより排気できないので出力P0発生せず.
方向制御弁 (ばね付)	ソレノイド焼損	0	ソレノイドが励磁できなくスプールが動作しないため, 圧縮空気の流れる方向が切換わらないので，出力P0発生せず.
	バネ折損	ϕ	ソレノイドが励磁されスプールが動作した場合ばねは伸びた状態で出力P0を生じ, ソレノイドの励磁がOFFされたときスプールが自動復帰できなくなり, 圧縮空気の流れる方向が切換わらないので出力P0が発生した状態で停止する.
	スプール固着	0	ソレノイド非励磁状態 : ソレノイドが励磁されても, スプールが固着して圧縮空気の流れる方向が切換わらないので，出力P0発生せず, ソレノイド励磁状態 : ソレノイドが非励磁になっても, スプールが固着して圧縮空気の流れる方向が切換わらないので, 出力P0発生し続ける.

（表 3.6　続き）

スピード コントローラ	ごみ詰まり	0	シリンダ前側から排気される圧縮空気が排気ポートからマフラを通るときごみ詰まりにより排気できないので出力P0発生せず.
エアシリンダ	ピストン固着	φ	圧縮空気がチューブ内に入っても, ピストン固着しているので出力P0発生せず.圧縮空気注入状態では出力P0は発生しつづける.
	ロッドパッキン割れ	φ	割れ箇所から圧縮空気の漏れ, 割れの大きさによっては，P0は発生するが圧縮空気の圧力，流量が不足して動作が鈍い.
	チューブ破壊	0	破壊箇所から圧縮空気の漏れ，出力 P0 発生せず.
（　外国文献調査例　約 60 例，および実施例 220 件　） ＊表中の論理値は P1,P0 で出力する 1，出力しない 0 を示し，φについては危険側故障障害の可能性を意味する.			

3.4　空気圧システムの FMEA と BIA 報告との比較

本研究で行っている空気圧システムのFMEAの結果について故障モードの偏りが無いか検討する必要がある．そのため，表 3.7 の，各々空気圧制御システムのザンクト・アウグスティン同業者組合労働安全研究所（BIA）[(10)] 報告（BIA-Report6/97e）の文献集よる危険源例と表 3.6 および付録 1 の関係する故障モードについて比較を行ったが用語の違いによる程度であり，本質的な違いはない.

表 3.7　空気圧コンポーネントにおける危険源例

障害モード（危険源）	方向制御弁	逆止弁	流量弁	圧力弁	配管	ホース関連	接続要素	シリンダ	圧力供給装置	圧縮空気処置			アキュムレータ	モータ
										フィルタ	オイラ	マフラ		
スイッチング時間の変動	○	○												
スイッチング停止位置の固着/不完全な開閉	○	○ (開閉不良)												
初期スイッチング位置の変動	○	○												
漏れ／割れ／外れ	○	○		○		○	○ (パッキン不良)							
漏れによる体積流量変動	○	○	○	○										
弁箱のひび割れ，稼動部分の破損，ねじの破損／外れ，カバーの外れ	○	○	○	○			○ （ねじ）	○ (圧力室)	○ (圧力室)	○ (筐体)	○ (筐体)	○	○	○
シャトル弁の出力接続が同時閉塞		○												
調整装置の変動,			○	○ (圧力制御)							○ (油量)			○
調整装置の操作要素の緩み			○	○							○			
比例圧力弁での制御値変動				○										

（表 3.7　続き）

設定圧超過，低下時の開放不可/閉鎖不可				○										
接続要素の破損					○									
詰まり					○	○	○			○		○		
プラスチック製でのねじれ					○									
破裂・破損，取り付けの外れ						○				○		○	○	○
圧力室の密閉不良								○	○					
最終状態減衰の故障														
ピストン･ロッドの折れ								○						
ピストン／ロッド，ピストン／機械間の結合解除								○ (カバー)						
バイパス弁の不良										○				
汚染監視／表示装置の故障										○				
圧縮空気での吸引流の変動														○
気体側の給気弁の故障														

＊パイロット式は別途評価すること
＊＊電磁弁の場合コイルの断線故障と端子間短絡故障を考慮すること．さらに，電磁リレー利用時は電気接点間の溶着故障と接触不良を考慮すること

3.5　空気圧システムの FMEA と ISO13849-2 の比較

3.4 項と同様の目的でISO13849-2 の付属書B（空気圧システムの妥当性確認ツール）[11] との比較，検討を行った．ISO13849-2 では基本安全原則，十分に吟味された安全原則，空気圧システムの各種機器における障害の一覧と障害の除外について規定されており，その一例を表 3.8 に示す．このISO13849-2 とは用語の違いによる程度であり，本質的な違いはない．

表 3.8 ISO13849-2 における障害一覧と障害の除外の例

機器名	考慮する障害	障害の除外	注記
方向制御弁	切り替え回数の変化	作動力が十分である限り，可能なコンポーネントにおけるポジティブな機械動作の場合には可能	—
	切替えられない（終端又はゼロのポジションで止まっている），または切り替えが完了してない（動作途中の任意の場所で停止してしまう）	作動力が十分である限り，可能なコンポーネントにおけるポジティブな機械動作の場合には可能	—
	最初の切り替えポジションが自発的に変更されてしまう．（入力信号なく）	保持力が十分である限り，稼働コンポーネントにおけるポジティブな機械動作の場合には，可能． 又は十分に吟味されたスプリングが使われており，かつ，正常な据付および運転条件が適用されている場合には，可能．	（1）正常な据付および運転条件が適用される場合とは， ・製造者が規定した条件が監視され ・可動部品の重量が，安全上適切な状態で稼働している（水平な据付など）のほか，

（表 3.8 続き)

	漏れ	スプール形のバルブで，ゴム製シールが取り付けられていることで十分な結合部分（重複部分）が得られている場合で，かつ，正常な運転条件が適用され，圧縮空気の処理およびろ過が十分になされている場合には，可能.	(2) ゴム製のシールがついたスプール形のバルブの場合には，ろ過による影響はほぼ解決することができる．長時間少量の液漏れが発生している場合を除く． (3) 製造者が条件を規定している場合には，通常の運転条件を適用する.

3.6 安全性確保上からの FMEA の限界

（1）FMEA は，基本的に故障モードの影響分析に対してシミュレーションを必要とする．しかし，現実には，システムの破壊効果など，シミュレーションを実施でない場合が存在する．その場合，数学的解析に基づく実証や計算機支援に基づくシミュレーションに頼らざるを得ないが，計算機支援によるシミュレーションの場合，シミュレーション自体の誤りを考慮しなければならなくなる．むしろ，この正しさの立証の方が難しくなってしまう．

（2）図 3.5 で故障モードの影響解析を行う場合，分析対象の規模が大きくなるほど，多重故障モード（2 重，3 重の故障モード）の影響分析が困難になる．この原因はFMEAにブロックの分割基準が存在しないからである．国際安全規格では，ブロックの分割をブロック間の独立性に求めており，この独立のブロックと“モジュール”と呼んでいる．本論文では，この分割点は，例えば動力供給系と制御系のインタフェースとし，それを改めてインタロックの一つとして定義する．通常，モジュールは“認証済みモジュール”として利用される．国際安全規格では，独立したモジュール間には単調論理の安全原則の成立が求められる [(12)] ．

3. 7　小括

本章では，空気圧駆動システム代表的構成例を構成する各種，空気圧コンポーネント（13 種類）について FMEA（Failure Mode and Effects Analysis）を実施して故障時の挙動について分析を行った．その結果，システム内部の圧力が上昇する側，低下する側の両側に危険側故障の原因となる故障モードが存在することが分かった. それは図 3.1 の P1, P0 における圧力の上昇，低下として現れる．

この解析した結果について BIA-Report6/97e と ISO13849-2 の付属書 B（空気圧システムの妥当性確認ツール）との比較を行い故障モードの偏り等について検討を行い本質的な違いが無いことを示している．

したがって，現状のシステムでは圧力上昇側の誤り（危険側誤り）を生ずるコンポーネントの存在を示すとともに, 圧力低下側にも危険側故障が存在するため空気圧駆動システムにおける故障監視には，窓特性による圧力の上昇（危険側誤り）と低下の両方を検出する監視の必要性がある．

さらに，危険側故障の原因となる故障モードが（例えばコンポーネントの破裂）発生した場合に動力供給が行われていた場合に破裂時の破片や噴出した圧縮空気が危険源となるため動力供給を遮断するインタロックシステムが必要である．

すなわち, 空気圧駆動システムにおける危険側故障に対する安全システムは圧力の上昇側と低下側にしきい値を持つ窓特性による監視を設け, しきい値の内側であることが確認できれば動力供給を行い, しきい値の外側またはしきい値の内側であることが確認できない場合に動力供給を遮断する機能が必要である．これは安全（確認）の原理を適用したインタロック（動力遮断・排気）であり，本質的に危険源（動力）を解消するインタロックシステムが必要である．

第 3 章　参考文献

（1） 小野寺勝重 著，“実践 FMEA 手法”，第 12 版(2007)，pp.2，日科技連.

（2） 中村瑞穂,田中慎也，杉本旭，“空気圧駆動システムにおける危険側故障を解消するためのインタロックの提案”,日本機械学会論文集 C 編, Vol.79, No.805(2013-9), pp.167-177.

（3）小野寺勝重 著，“実践 FMEA 手法”，第 12 版(2007)，pp.6，日科技連.

（4）小野寺勝重 著，“実践 FMEA 手法”，第 12 版(2007)，pp.13，日科技連.

（5）中村泰三，榊原哲　著，“やさしく学べる信頼性手法”，第 2 版（2005），pp. 71, 日科技連.

（6）小野寺勝重 著　“FMEA 手法と実践事例”，第 1 版(2006)，pp.63-65，日科技連.

（7）小野寺勝重 著　“FMEA 手法と実践事例”，第 1 版(2006)，pp.2，日科技連.

（8）小野寺勝重 著　“FMEA 手法と実践事例”，第 1 版(2006)，pp.56，日科技連.

（9）小野寺勝重 著　“FMEA 手法と実践事例”，第 1 版(2006)，pp.53，日科技連.

（10）BIA-Report 6/97e，Categorized for safety-related control systems in accordance with EN954-1(1999)，HVBG.

（11）ISO13849-2:2003，Safety of machinery-Safety-related parts of control systems-Part 2:Validation(2003)，International Organization for Standardization.

（12）中村瑞穂　著，“平成 18 年度　長岡技術科学大学工学研究科　修士論文　油圧・空気圧制御システムの動力供給に対するインタロックの検討”，pp21

第4章 空気圧駆動システムの危険側故障を解消するインタロックシステムの提案

4.1 はじめに

本章では, 前章で行った空気圧システムの圧力調整に伴う危険側誤りに関する調査結果に基づき, そのリスクを解消するインタロックの実現可能性について論理的な検討を行い, その結果窓特性を有する監視によってフェールセーフ・インタロックが実現し得ることを示す.

第 4.2 節では, 空気圧駆動システムにおける圧力制御がフェールセーフの条件（安全（確認）の原理に基づくユネイトな論理的関係）を満たすか否かを検討する. その結果, 空気圧システムの動力調整部に注目し, 駆動系との分離点に圧力の上昇と低下を検出する窓による監視（以降, “窓監視”とする）を行うことにより, 危険側誤りの発生を動力供給の遮断によって回避するインタロックが実現可能であることを示す.

第 4.3 節では, 危険側誤りを監視するセンサについて述べ, これを窓監視に用いたインタロックが, 国際規格 ISO13849-1 による安全要求を満たすウインドゥ・コンパレータを用いて達成可能であること, そして第 4.4 節では危険側誤りに対する出力遮断特性（ユネイトな論理的関係）について論理的な検討を行い, 窓監視によるインタロックを導入した空気圧駆動システムの特性と効果について述べる.

第 4.5 節では出力遮断に用いる遮断弁の構造や動作について述べ, 第 4.6 節ではインタロックシステムの構成と動作について述べており, インタロックシステム自身が故障した場合に安全側停止が実現される構成であることについて示す.

なお, 本章では, “危険側誤り”という場合と“危険側故障”という場合があるが, 基本的に, 操作（制御）の場合「誤り」, コンポーネントの場合「故障」として区別する.

4.2 動力調整部の窓監視の構成

図 4.1 における空気圧駆動システムは, コンプレッサ, 圧力容器等からなる「動力供給部」, レギュレータによって空気圧駆動システムが動作するのに必要なレベルの圧力

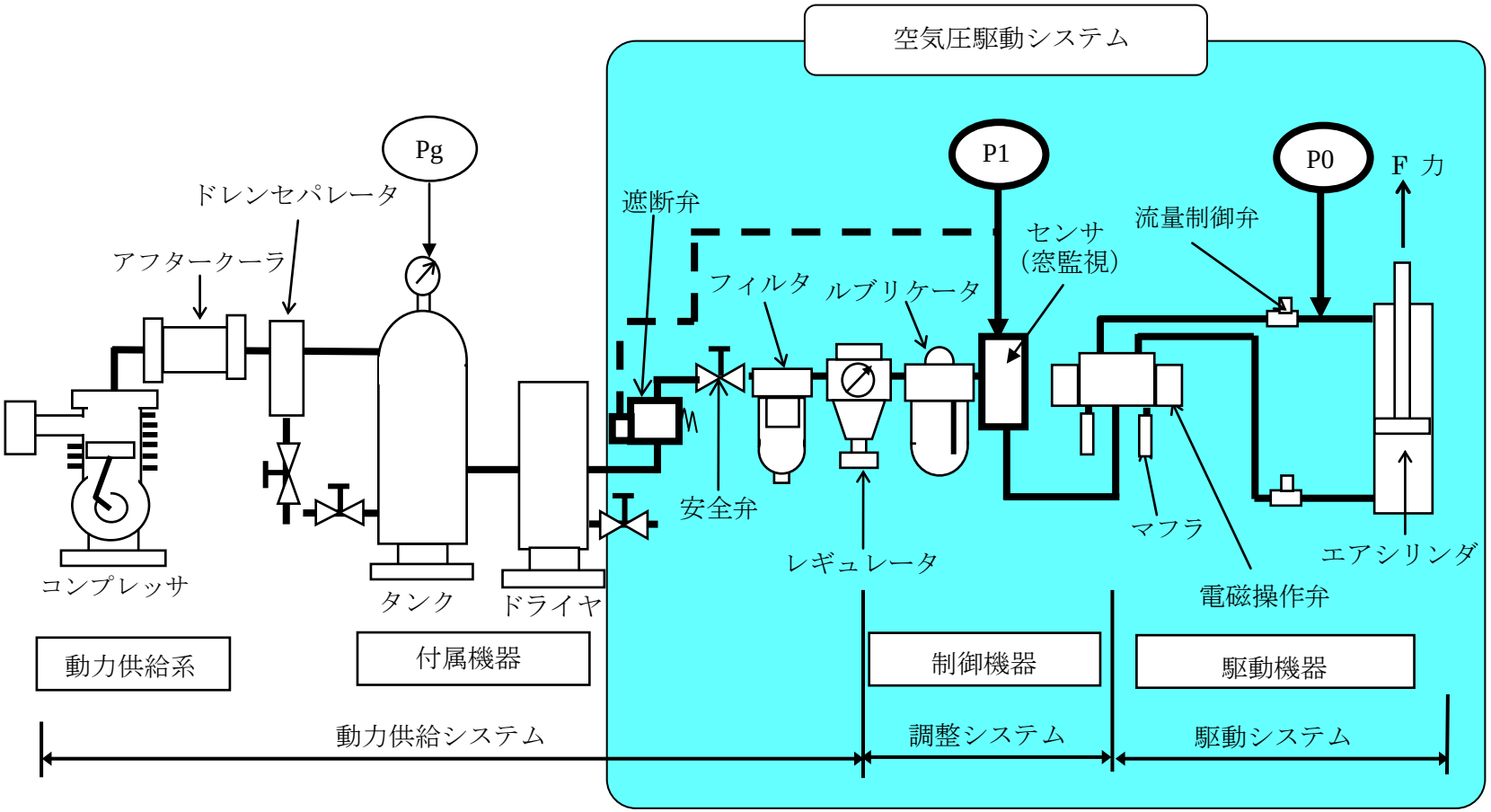


図 4.1　空気圧駆動システムの構成例

調整を行う「動力調整部」，制御機能および作動機器で構成される「駆動系」の大きく 3 つに分けられるとし，改めて，動力供給部出力を Pg，動力調整部出力を P1，駆動系出力を P0 とおく．空気圧駆動システムとは図 4.1 の網掛けの部分であり，本章で提案するインタロックシステムにおいて防護する範囲でもある．一般に Pg はユーティリティとして共通に使用される圧力源であり，少なくとも調整された Pg を負荷とするシステムコンポーネントはストレングス（強度 Pst）を Pst＞Pg の条件で設計されるべきと考えられて当然である．さらに，危険側誤りを最悪の無調整状態 Pgmax と想定して Pst＞Pgmax を確保するコンポーネントを選択・使用すれば，Pg 調整の危険側誤りに対する故障監視を不要とすることができる．ただし故障特性 Pgmax は，レギュレータ入口部まで適用される．さて，動力調整部圧力 P1 は，レギュレータによって動力源 Pg を調整して，規定圧力 P1max を超えない条件で生成される 2 次的動力源であると言える．この調整（安全の調整操作）には少なくとも危険側の誤りが許されないのは，P1max を超える負荷に耐えられないコンポーネントがローカルに存在するにも拘らず，危険側の誤りによって無調整状態 Pgmax の負荷が生じ得るからである．

ここでは負荷を受けるコンポーネントをエアシリンダで代表させているが，駆動系内圧力P0はエアシリンダを動作させて仕事（目的操作）をするための圧力であり，元圧Pgをエアシリンダにより仕事に必要な圧力値をPg≧P1≧P0の条件でレギュレータにより調節して設定される．ただし，P0はエアシリンダの動作を行うため圧力の変動が大きい．論理的検討のために，まず，P1およびP0を，各々出力が存在するとき論理値1，不在であるときを0とする2値の論理変数で表す．動力調整部と駆動系は独立して，異常状態が相互に影響しない関係にあるとすれば，本来，理想的なフェールセーフ・システム[(1)，(2)]として，次のような単調（ユネイト）な論理的関係が成立する[(3)]．

$$P1 \geqq P0 \tag{4.1}$$

ここに式（4.1）は，P1=0とP0=1の組み合わせだけは生じない関係，すなわち「少なくとも，入力P1が不在（P1=0）の場合，出力は発生しない（すなわちP0=0）」とする論理的関係を示す．駆動系P0=1は動力調整部P1=1に基づいて出力され，安全な駆動系出力P0=1を確保するには，少なくともP1=1には危険側誤りが含まれないことが条件である．フェールセーフは，安全（確認）の原理[(4)]に基づき，P1の危険側誤りに対してP1=0→P0=0の処理を行って危険な出力を生じないことを要請する．なお，図4.1では動力調整部圧力P1および駆動系圧力P0はアナログ出力であるが，式（4.1）はこれを2値の論理変数としているので注意を要する．

図4.1のシステムでは，動力調整部で過圧が生じたとき（例えばサージ圧），その過圧は直接駆動系に伝達される．駆動系に過圧が生ずる故障は危険側故障と判断される．あるいは，駆動系の，例えば方向制御弁に目詰まりが生じたとき，あるいは，アクチュエータを強制的に動かした場合，その影響は動力調整部出力P1の上昇となって現れ，結果として駆動系が過圧（危険側故障）を生ずる．このように，動力調整部と駆動系とは，現状では必ずしも技術的独立性を達成していない．このため図2.3のシステムには式（4.1）を満たすための処置を本来必要とする．すなわち，動力調整部と駆動系を分離した場合，纏めると，以下の問題点が生じる．

① 駆動系の故障で動力調整部に過圧が発生する．

② 動力調整部で発生した過圧は直接駆動系に伝達される．

上述の問題点は①および②のいずれも，駆動系入力P1において過圧の症状となって現れることになる．一方，FMEAで示されたように，動力調整部では出力P1の低下となって現れる故障モードが圧倒的に多い．この圧力低下には，コンポーネントの故障によって，例えば割れによる空気の大量噴出など，即時遮断を要する事態も含まれている．よって，動力調整部出力P1（すなわち，駆動系入力）の監視には，この出力P1が上昇しても，低下しても異常を通報することのできる監視が不可欠となる．この監視を，改めて，“窓監視”（あるいは窓による監視）と呼ぶことにする[(5)]．

この，“窓監視”の監視結果が動力調整部または駆動系のコンポーネントの故障により上限／下限のしきい値から外れた場合には即時に動力を遮断するインタックを構成するが，その設置位置は「割れ」の故障モード（下限のしきい値）の場合に対する動力遮断の要請から図4.1の電磁式遮断弁（以降，“遮断弁”とする）をレギュレータの入口部に設置する．本論文で提案する“窓監視によるインタロック”は後に示すように，フェールセーフな窓監視のためにウインドゥ・コンパレータ[(6)～(10)]が適用可能である．

4.3 窓監視の実現法

4.3.1 ウインドゥ・コンパレータの定義[(6)～(10)]

電子回路の演算発信回路は，入力電圧Vがあらかじめ定められた範囲内（$V_L \leqq V \leqq V_H$）にあるときに限って交流信号を出力し，それ以外のときは交流信号の出力を停止させる回路を言う．あらかじめ定められた範囲が一種の窓（ウインドゥ）と考えられ，この窓との比較（コンパレート）を行うことから，ウインドゥ・コンパレータと呼ぶ．図4.2は，オペアンプの出力をフェールセーフなウインドゥ・コンパレータでレベル検定して，回路全体としてフェールセーフな特性を持たせようとするものである．図の回路では，オペアンプは約100倍の増幅度を持っているため，オペアンプの入力が100mVから

130mVまで変化したとき，オペアンプの出力は10V（=V_L）から13V（=V_H）まで変化する．この出力をフェールセーフなウインドゥ・コンパレータに入力することによって，150kHz前後の交流出力を生じる．ただし，この場合，ウインドゥ・コンパレータに印加される電源電圧はこれよりも低い電圧（この場合+8V）でなければならない．

一方，オペアンプの出力Vが$V_L \leqq V \leqq V_H$なる範囲から逸脱したとき，ウインドゥ・コンパレータから出力されていた交流信号は停止する．また，オペアンプの基準入力電位V_Bを設定するための抵抗Raが断線したときは，V_BのレベルはV_Hより高くなり，Rbが断線したときはVaのレベルはV_Lより低くなる．さらに，入力抵抗Rinが断線するとオペアンプの出力はV_Lより低くなる．さらに，入力抵抗Rinが断線するとオペアンプの出力はV_Lより低くなり，帰還抵抗R_fが断線するとオペアンプの出力はV_Hより高くなる．そして，いずれの場合にも，ウインドゥ・コンパレータから出力されていた交流信号は停止する．以上により，図4.2の回路では，オペアンプの出力Vが$V_L \leqq V \leqq V_H$からなる範囲から逸脱したときだけでなく，Ra，Rb，Rin，R_fのいずれかに断線が起きたときでもウインドゥ・コンパレータから出力された交流信号は停止するから，フェールセーフな特性が確保できる．このように故障が危険側誤りになる特性を「非対称故障モードを有する」と表現する．

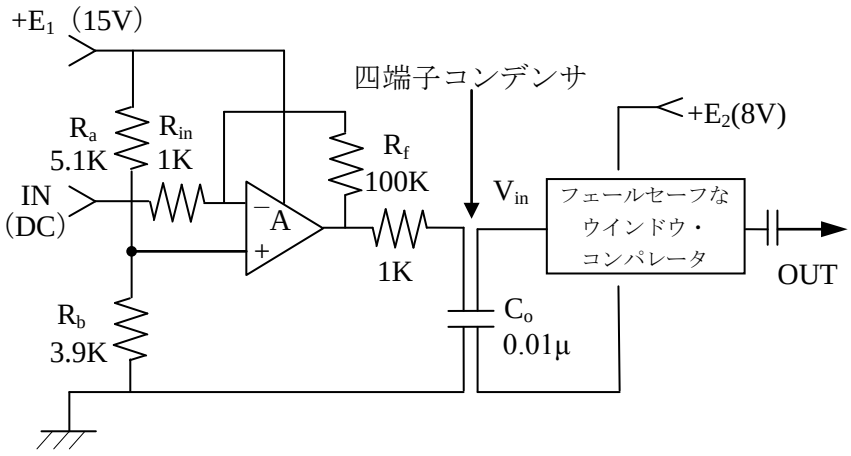


図4.2　フェールセーフウインドゥ・コンパレータ

4.3.2　ウインドゥ・コンパレータの論理的表現

ウインドゥ・コンパレータは，入力レベルVに対して二つの異なるしきい値V_H，V_L（$V_H>V_L$）をもち，この二つのしきい値間の内側と外側で異なる論理値の2値出力F(x)∈{1,0}を発生するものとする．すなわち，次式で定義される．

$$F(x) = 1,\ V_L \leqq V \leqq V_H \qquad (4.2)$$

$$= 0, \qquad V < V_H\ , \qquad \text{または} \qquad V > V_L$$

また，上記のウインドゥ・コンパレータの動作状態を Q*とすると，動作状態を含む出力関数 H(x)∈{1,0}が次式で表されるウインドゥ・コンパレータをフェールセーフなウインドウ・コンパレータと呼ぶ.

$$H(x) = F(x) \cdot Q^* \qquad (4.3)$$

ここに，二つのしきい値の間隔をV_H-V_Lをウインドゥ・コンパレータの窓と呼ぶ．そして，(4.3) 式はフェールセーフなウインドゥ・コンパレータとして故障時出力はH(x)=0となる.（(社) 日本労働安全衛生コンサルタント会編，これからの安全技術，(2000.1)，pp81-82 を引用・要約.）

4.3.3　窓監視の構成

制御安全に関する国際規格ISO13849-1[(11)]で示される要求事項を，窓監視から動力供給遮断までに適用すれば以下のようになる. 動力調整部出力P1に対する窓監視出力および動力遮断のための出力を各々2値の論理変数Q1およびQ0とし，非遮断時における，各々窓監視出力，遮断出力の状態を論理値1，遮断時における，各々窓監視出力，遮断出力の状態を0とおく．ここに，遮断出力Q0は非遮断出力状態を論理値1とする点に特に注意が必要である．この入出力の関係には式（4.1）と同様に次式のユネイトな論理的関係が要請される [(3)] .

$$Q1 \geqq Q0 \qquad (4.4)$$

ただしQ0は，図4.1のレギュレータ入口に設けた遮断弁の操作指令であり，非遮断出力Q0はP1が正常であるという条件（P1≧Q0）で生成する．したがって，P1が正常でないとき，特に危険側誤りは，Q0=0による遮断とともに外部への排気の処理がなされる．式（4.4）において，P1に対する窓監視に基づく出力Q1は，窓の上限のしきい値をThu，下限のしきい値をThdとおけば式（4.5）で表される．

$$Q1 = 1 \quad ; \qquad Thu \geqq P1 \geqq Thd \tag{4.5}$$

$$= 0 \quad ; \qquad P1 \geqq Thu \quad \text{または} \quad P1 < Thd$$

式（4.5）により，「動力調整部出力P1が窓内にない（正常でない）のに，非遮断出力（Q0=1）を生じてはならない」とする論理的関係が実現する．ただし窓監視が式（4.4）の単調（ユネイト）な論理関係を満たすには，国際規格ISO12100-1[(11)]で求められる非対称故障モードの特性を有しなければならない．誤りが本質的に危険側誤りとならない条件を物理的特性（非対称故障モード）によって達成するのはフェールセーフ設計の基本だが，本論文で論ずるインタロックでは，危険側誤りで危険な出力が生ずる前に動力を遮断して，システムとして非対称故障モードを実現するものであり，窓監視手段だけでなく，4.4項で詳しく述べるように，動力遮断の非対称誤り特性（フェールセーフ）を考慮することが重要である．

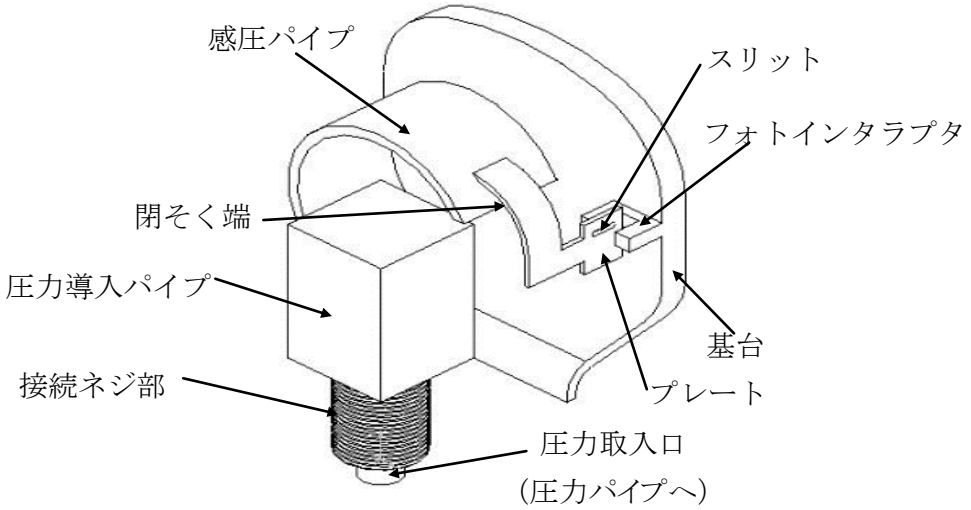
また，窓の上限のしきい値Thuは規定圧力P1maxを考慮した設定がなされるが，下限のしきい値Thdも，割れによる空気の噴出等の異常を考慮し，設計において慎重に決定すべきであろう．

圧力P1の窓監視を行うためのセンサを図4.3に示す．これは，ブルドン管のパイプの先端にスリットを備えて，フォトインタラプタでスリットを通過する光を検知している間，動力調整が正常に維持されていると見なし，「安全」の判断を示す出力（Q1=1）を生成し，スリットの範囲内にない場合Q1=0となるように構成した窓監視手段である．

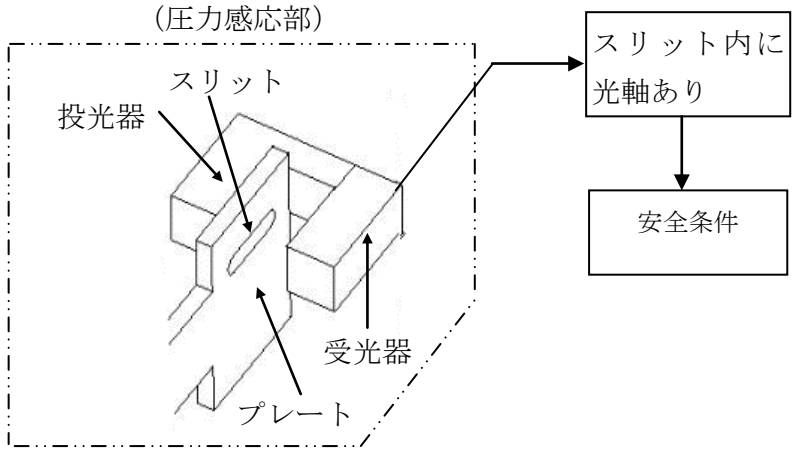
ひずみゲージを用いて窓監視（上限／下限のしきい値）を行う方法も検討したが，ブリッジバランスが不安定であること等を考慮して，窓を固定したスリットとし温度安定性に優れたフォトインタラプタを用いる方法を用いた．圧力の正常性確認にブルドン管を用いる方法については別途報告するが，上限／下限のしきい値による窓特性を持つ判断回路（フェールセーフ演算発信回路）として既にウインドゥ・コンパレータが活用されているので本論文では信号処理に当該回路を用いる．

ウインドゥ・コンパレータを用いると，図4.3で要請されるように，圧力低下のみな

らず，過圧状態も同時に監視できる特徴を備えることができ，しきい値をもつので動力調整部出力P1を2値化できる．なお，ブルドン管に潜在する危険源には，ブルドン管の外れ，ブルドン管の目詰まり，ブルドン管の腐食・漏れ，ブルドン管の折れ・曲がり，ブルドン管の破損・破裂・破壊，導圧管の目詰まり，腐食，固着等が考えられる．ここでは詳細な検討は避けるが，ブルドン管に関わる故障は，その殆どがスリットを通過する光量を低下させ下限のしきい値でチェックされると推測される．さらに，表4.1に圧力計の危険源例を示す．また，このセンサが取り付けられる周辺環境を図4.4に示す．



（a）圧力監視センサ



（b）監視部分拡大図

図4.3　窓監視手段（ウインドゥ・コンパレータ）[13]，[14]

表 4.1　圧力計の危険源例 [15]

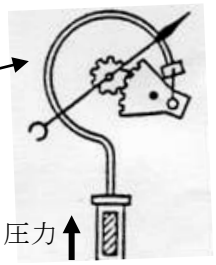
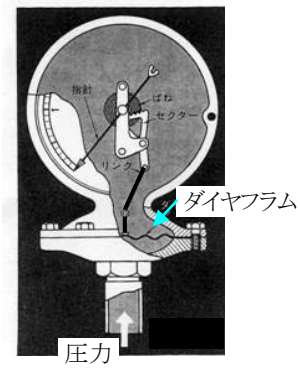
センサ		危険源
圧力計	ブルドン管 圧力の大きさにより円弧の曲率半径が変わる  	1.ブルドン管の外れ 2.ブルドン菅の目詰まれ 3.ブルドン菅の腐食，漏れ 4.ブルドン菅の折れ曲がり 5.ブルドン菅の破損，破裂，破壊 6.導圧菅の目詰まり，漏れ，腐食，固着 7.針のひっかかり，外れ 8.針駆動機構の固着，外れ，緩み，摩耗
	ダイヤフラム （弾性膜）  	1.膜の外れ 2.膜の変形 3.膜の材質変化 4.膜の破損，破裂，破壊 5.膜の水素透過，脆化，腐食，異物の付着 6.導圧菅の目詰まり，漏れ，腐食，固着 7.針のひっかかり，外れ 8.針駆動機構の固着，外れ，緩み，摩耗

図4.4　空気圧駆動システムの周辺環境

4. 4　出力遮断の方法

4.4.1　インタロックシステムの論理的表現

空気圧コンポーネントの故障により増大するリスクに対処するには，本論文では窓監視によって故障を検出して動力を遮断する方法を提案しているが，非対称故障モードの要求から，インタロックはユネイトな特性で構成されなければならない．それは，危険側誤りの防止のために導入したインタロックが改めて危険側誤りを生ずる可能性があるからである．

図 4.5 に，運転命令Mに許可を与えるために，安全の確認に基づいて作業実行の出力エネルギーが生成される一般的な構成をインタロックモデルで示す[14]．ここに安全条件Siと運転命令Mの関係は，論理積機能&*で表してある．同図は安全条件Si，運転命令M，機械の運転出力Sは，各々，存在時を 1，不在時を 0 とする論理変数で表し，さらにインタロック機能（論理積機能）&*を正常動作時 1，正常でないとき 0 とすれば，機械の運転出力Sは式（4.6）で示される．

$$S = Si \cdot M \cdot \&^{*} \qquad (4.6)$$

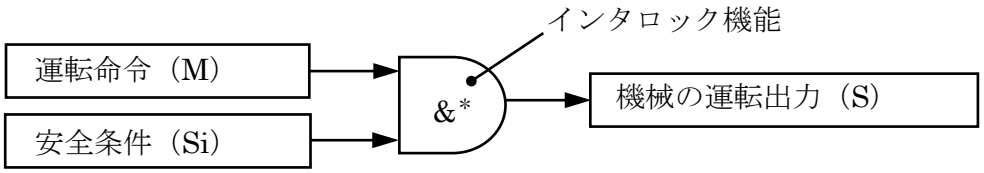


図 4.5　安全作業インタロック[14]

式（4.6）には表されていないが，本来，動力源は，危険な時に遮断の要求に確実に応えると言うように，安全制御上重要な役割を果たす．図 4.6 に，安全条件 Si の許可に基づいて動力供給出力 P1 が機械の運転出力 S として出力される実用の設備として，本来要請される構成をインタロックモデルで示している．同図は動力供給設備に故障が生じたとき，その動力供給 P1 が必ず遮断される条件を P1*とし，これを動力供給設備の正常性としている．

一般機械を表す図 4.6 では，動力供給出力 P1 を，その動作状態を含めて P1*（=P1・P1*）として示してある．
改めて，P1*は動力供給設備の正常性を示す論理変数であり，正常状態（P1*=1）は，いつ故障しても動力源を遮断できるという条件でインタロック機能に動力が供給されることを意味する．逆に，P1*=0 は，動力供給設備の故障による動力源遮断 P1=0 を意味する．これらを考慮すると，一般に，機械の運転出力 S は式（4.7）で示される．

$$S = Si \cdot M \cdot P1^{*} \cdot \&^{*} \qquad (4.7)$$

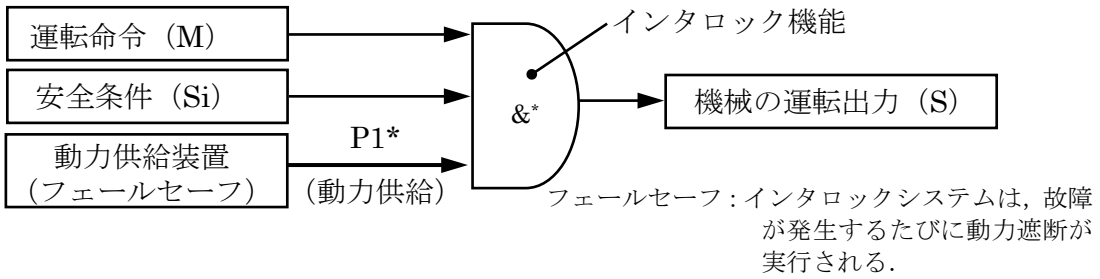


図 4.6　動力供給の安全性を備えた安全作業インタロック（フェールセーフ機能）[16]

4.4.2　故障時の動力源遮断の正常特性

図 4.7 に，本論文で対象とした空気圧駆動システムのフェールセーフ・インタロックを示す．本来，安全の条件は，駆動系のコンポーネントの強度（ストレングス）に関わる負荷 P0 の条件として生じるが，システムの実行に伴う P0 の変動が大きいため，安定した 2 次的動力源 P1 を生成して，これにより監視が可能となる．安全な動力源 P1 は，安全条件に基づき，レギュレータによる正常な操作（図 4.6 の操作 M）で作られ，窓監視による正常性の確認（図 4.6 の Si）によって認められ，さらに，遮断に対する動力源の条件 P1*を揃えてやっと，出力 P0 への伝達可能な動力源が生成される．
また，式（4.5）の Q1 は 2 次的動力源 P1 に対する窓監視出力であり，Q1=1 の時に図 4.1 の遮断弁が非遮断（Q0=1）であることを示している．すなわち，インタロックで遮断弁（図 4.1）に対する非遮断の要求はレギュレータで調整が正常であることを示し，よって Si（安全条件）とすることができる．
なお，起動時は P1 の圧力が不在であり Q1=0 であるため起動できない．一般的に安

全確認システムでは起動時において「安全」が確認されていない状態であり，機械が安全確認できる状態まで「人間」が持っていく．すなわち，起動時の安全確認は「人間」に委ねられることになる．

図 4.6 は，安全上のトラブルをすべて動力源の異常と判断している点に特に注意が必要である．危険側誤りの検知は勿論，検知手段に故障を生じた場合も動力源を遮断する構成となる．そのため，動力源遮断の正常性P1*が動力源P1 の条件となっている．現実の動力遮断（P1*=0）のために，例えば，動力遮断に用いる遮断弁（図 4.1）は，電磁力を供給して弁を「開」とし，電磁力を失ったときバネ力で弁を「閉」とし，確実に動力を遮断できるノーマル・クローズ構造 [17] とし，いわゆる「ブラ」の状態を許さない条件を要求する．これらを纏めると，安全条件Siを 2 次的動力源P1 に対する窓監視出力をQ1（Si）で表し，機械の運転出力Sを動力源P1 として 2 次的動力源出力をP1（S）で表すと，図 4.7 の空気圧駆動システムのインタロックは式（4.8）で示される．

$$P1(S) = Q1(Si) \cdot M \cdot P1^{*} \cdot \&^{*} \qquad (4.8)$$

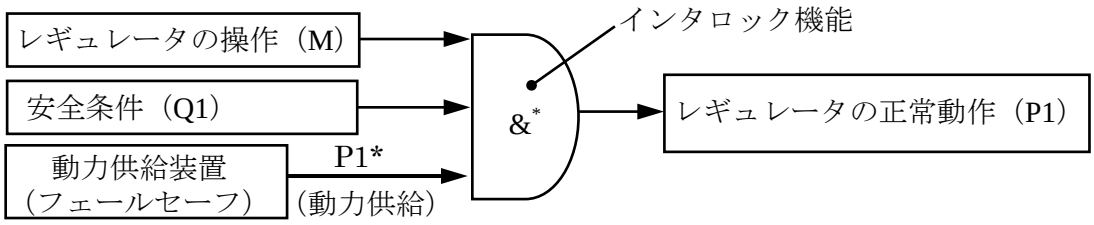


図 4.7　空気圧駆動システムのフェールセーフインタロックシステム [18]

4.4.3 一般的出力遮断と安全弁の役割

一般に，安全の制御には，まず，安全を調整する能動的機能が存在する [19]．事故は，調整を誤った状態で実行される行為によって発生する．安全の調整操作（図 4.6 のMに相当する）と事故の可能性のある目的操作 [20]（P0 による仕事）という 2 つの操作（制御）がユネイトな論理的関係（すなわちM≧P0）で実行されることで理想的な安全制御システムが実現されるという見方もできよう．しかし，人の行為はもとより，安全の調整は空気圧の場合レギュレータによるところであるが，どのような手段でも，機能が能

動的である限り基本的に誤りが避けられないため，程度の差こそあれ，確率の制約（リスク）を受ける．

失敗は避けられないとしながらも，安全の調整には失敗が許されないとする非現実的状況では，調整の結果（安全）を改めて確認して，確認結果に基づいて事故の可能性のある行為を行うようにして，事故の可能性自体を解消する以外にはないと言える．しかし，その場合の深刻な問題は，安全が確認できないとき行為を確実に停止できるか否かである．

現実には，図 4.6 は，フェールセーフな圧力調整出力特性（P1*）を達成する代わりに，図 4.7 に示すように，レギュレータに安全弁（さらに，逃し弁，減圧弁，ラプチャーディスク等）を併用してフォルトトレラント・システム [21] を構成している場合が多い．安全弁の併用は，レギュレータの調整誤りのためのインタロックに位置づけられると思われがちだが，安全弁には（列記した他の手段も）動力源を遮断する機能はなく，安全の調整を助けるリリーフ機能である．ただし，安全の調整が異種の手段であるため，式（4.9）に示すように，多様系（ダイバシティシステム）[22] によるフォルトトレランスと見なすことができる．

なお，図 4.7 の m1（安全弁），m2（リリーフ弁（逃がし弁）），m3（減圧弁），m4（ラプチャーディスク）は，調整操作を実行するリリーフ機能であり，各々，“調整機能が実行されている”を 1，“調整機能が実行されない”を 0 とする論理変数で表している．また式（4.9）は，フェールセーフな遮断構造を持たないものとして P1*の代わりに P1 と置いている．OR*は論理和判断の正常性を示す（必ずしもフェールセーフでない）．

$$P1(S) = Si \cdot \{(M \vee m1 \vee m2 \vee m3 \vee m4) \cdot OR^{*}\} \cdot P1 \cdot \&^{*} \qquad (4.9)$$

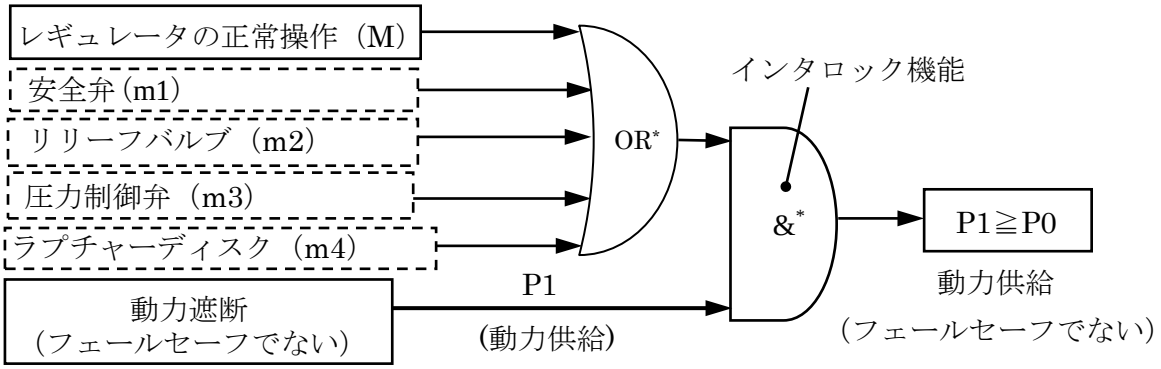
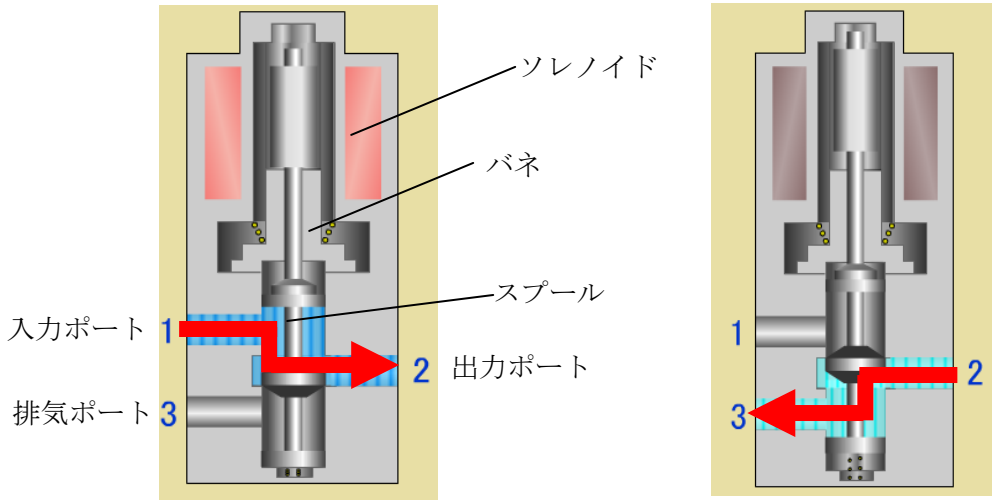


図 4.7 多様系フォルトトレランスシステムによるリリーフ機能 [5]

安全の調整手段が多様化されているので，Si＝1 となる確率が上がって P1=1 となる確率（稼働率）が上がる点で，多様系のフォルトトレランスとしての有効性が認められるが，危険側誤りの監視がなされておらず，また，正当な動力遮断構造を持たないためフェールセーフ・インタロックとは認められない．稼働率を指向するシステムとしての欠点があることが見逃されてはならない．

4.5　遮断弁

遮断弁は 3 ポート 2 位置ノーマル・クローズ型電磁式方向切換弁（図 4.8）を用いている．この弁は入力ポート，出力ポート，排気ポートの 3 つのポートがあり，通電時にスプールが動作して入力ポート→出力ポートに高圧空気が供給（動力供給）される（図 4.8（a））．非通電時にはスプールがバネにより戻り，出力ポート→排気ポートとなり動力遮断→排気となる構造である（図 4.8（b））．つまり，安全が確認されている場合（ウインドゥ・コンパレータから交流信号が ON の場合）に入力ポートから出力ポートに高圧空気が供給される．一方，安全が確認できない（ウインドゥ・コンパレータから交流信号が OFF の場合）または，遮断弁自身が故障した場合にバネよりスプールが戻り，入力ポートが閉（遮断）となり，出力ポートから排気ポートに高圧空気が流れて排気される構造である．すなわち，故障や交流信号が入力されなければ自動的に入力ポートから出力ポートに高圧空気が供給されない構造である．



（a）電源 ON 時　　（b）電源 OFF 時

図 4.8　遮断弁の構造と動作

4. 6　インタロックシステムの構成と動作

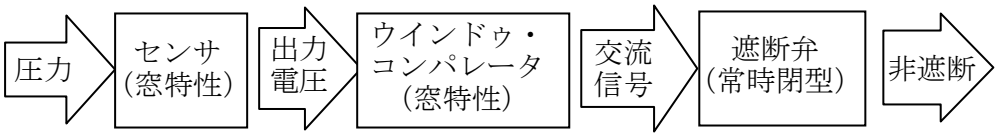
インタロックシステムはセンサ（図 4.3），ウインドゥ・コンパレータ（図 4.2），遮断弁（図 4.8）によって構成されている．図 4.9 にインタロックシステムの構成と動作を示す．図 4.9（a）は正常動作について示しており，P1 の圧力がセンサの窓の内側にあることが確認できたときに電圧が出力され，ウインドゥ・コンパレータに入力され，入力された電圧がウインドゥ・コンパレータの窓内にあることが確認されたら遮断弁に交流信号が出力され，ノーマル・クローズ型の遮断弁が ON となり非遮断となり動力供給が行われる．

図 4.9（b）ではセンサで窓の内側を確認できない，センサが故障した場合について示す．センサが故障または窓の内側に P1 が確認できないときはセンサから電圧が出力されず，ウインドゥ・コンパレータからも交流信号出力されないため遮断弁は OFF となり動力遮断が実行される．

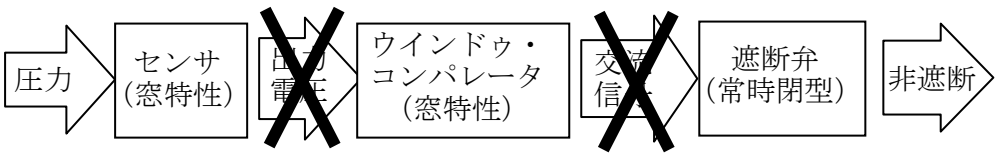
図 4.9（c）ではウインドゥ・コンパレータおよび遮断弁が故障した場合にウインドゥ・コンパレータはフェールセーフであるため交流信号が出力されず遮断弁が OFF となり，さらに遮断弁自らの故障についても OFF となるため動力遮断が実行される．

このように，インタロックシステムは自身が故障した場合に安全側停止が実現される構成となっている．

（a）正常動作



（b）センサで窓の外側の判断とセンサの故障



（c）ウインドゥ・コンパレータの故障と遮断弁の故障

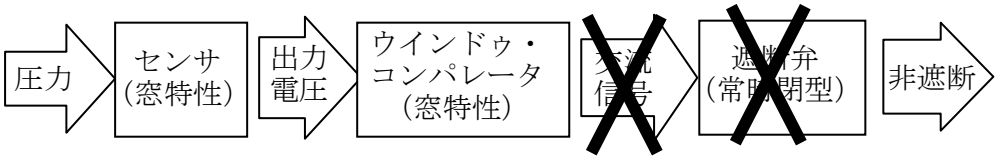


図 4.9　インタロックシステムの構成と動作

4.7　小括

安全の共通の原理に準拠したフェールセーフ・システムはユネイトな論理的関係で実現されるとされている．そこで，空気圧駆動システムの構成例を①動力供給部，②動力調整部，③駆動系に分離し，動力調整部に注目し駆動系との分離点における動力調整部圧力に対し上昇／低下を監視する窓監視を提案している．

窓監視によるインタロックを構成するため，本章では窓監視を可能とするセンサを開発し，これに ISO13849-1 による安全要求を満たすウインドゥ・コンパレータを適用して，ユネイトな論理的関係を条件とするフェールセーフ・インタロックの実現可能性を示した．また，フェールセーフは非対称故障モードによって実現されるとする ISO12100-1 の見方から改めて検討を加え，本システムがこの立場からもフェールセーフに矛盾していないことを明らかにした．フェールセーフ・インタロックの重要な条件である動力遮断の故障特性に関し，窓監視によるフェールセーフ・インタロックに備えるべき遮断構造について検討を行なった．

さらに，本システムは危険側故障が生じても安全側停止となるセンサ，ウインドゥ・コンパレータ，遮断弁によって構成されている．

また，機械安全の国際規格ISO12100-2[23]（例えば 4.11.5，4.11.6，4.12.2 項など）にほぼ準拠していると言える．

さらに機械の制御安全の国際規格 ISO13849-1 では安全関連部の危険側故障の発生確率の低減が要求されている（例えば 4.2 項）．本システムでは危険側誤りに対して動力を遮断しており，危険側故障の発生自体を抑制していると言える．

したがって，本章では危険側誤りの監視および動力遮断構造を持ち危険側故障の影響（危害）を抑制するフェールセーフインタロックシステムの提案を行っている．

第 4 章　参考文献

(1)　杉本旭，蓬原弘一，向殿政男，“安全作業システムの原理とその論理的構造”，電気学会論文集 D 編，Vol.107D，No.9(1987)，pp.1092-1098.

(2)　土屋誠治,“フェイルセイフ論理方式の研究”, 電気試験所研究報告, No.695（1969）

(3)　蓬原弘一，杉本旭，“安全確認形作業システムの論理的考察”，日本機械学会論文集 C 編，Vol.56，No.529(1990)，pp.60-67.

(4)　杉本旭, 蓬原弘一,“安全の原理”,日本機械学会論文集 C 編, Vol.56, No.530(1990), pp.75-83.

(5)　中村瑞穂,田中慎也，杉本旭，“空気圧駆動システムにおける危険側故障を解消するためのインタロックの提案”,日本機械学会論文集 C 編，Vol.79，No.805(2013-9)，pp.167-177.

(6)　蓬原弘一，向殿政男，“窓特性をもつフェイルセーフ論理素子を使ったインタロックシステムの一構成法”, 電気学会論文集 C 編, Vol.109, No.9(1989), pp.676-683.

(7)　蓬原弘一，杉本旭，向殿政男，“フェールセーフ・ウィンドゥ・コンパレータの構造とその応用”，第 18 回 FTC 研究会資料.

(8)　蓬原弘一，“非対称誤り素子によるフェイルセイフ論理回路の一構成法”，電気学会論文集 D 編，Vol.104，No.2(1984)，pp.29-34.

(9)　Futsuhara,K.,Sugimoto,N.,and Mukaidono,M.,“Fail-Safe Logic Elements Having Upper and Lower Thresholds and Their Application to Safety Control”, Digest of Papers of FTCS-18,Poster Session(1988-6,Tokyo).

(10)（社）日本労働安全衛生コンサルタント会編, これからの安全技術, 第 1 版(2000), pp.81-82，中央労働災害防止協会.

(11)　ISO13849-1:2006，Safety of machinery-Safety-related parts of control systems, Part1:General principles for design(2006)，International Organization for Standardization.

(12)　ISO12100-1:2003,Safety of machinery-Basic concepts and general principles for design, Part 1：Basic terminology，methodology(2003)，International Organization for Standardization.

(13)　安全技術応用研究会編，安全システム構築総覧，初版(2001)，p.55，株式会社通産資料調査会.

(14)　蓬原弘一，杉本旭，向殿政男，“安全作業システムにおけるインタロックの構造と実現”，電気学会論文集 D 編，Vol.107D，No.9(1987)，pp.1099-1106.

（15）蓬原弘一，“JIS B 9700-1（ISO12100-1）解説”，長岡技術科学大学システム安全系，初版（2007）
（16）Proposal of interlock System in Pneumatic and Hydraulic Control Systems（SISA2007）.
（17）杉本旭，蓬原弘一，“安全制御系における安全情報のエネルギー伝達”，日本機械学会誌 C 編，Vol.56，No.530（1990），pp.132-139.
（18） 中村瑞穂，田中慎也，杉本旭，“空気圧駆動システムの圧力制御における危険側誤りを解消するインタロックの提案”，2013 年度日本機械学会　産業・化学機械と安全部門講演論文集，pp.19-20.
（19）中村瑞穂，田中慎也，杉本旭，“安全制御の原理による圧力容器の安全システムの考察”，第 45 回安全工学研究発表会予稿集，pp.97-100.
（20）中村瑞穂，千葉正伸，杉本旭，“安全制御の原理による圧力容器の安全システムの考察”日本機械学会 2013 年度年次大会 DVD 論文集-S171014.
（21） 蓬原弘一,“安全関連基礎用語集 - 国際安全規格体系との絡み - ”, 初版 (2004)，pp.23
（22）関口隆，佐藤吉信監修，“（社）日本機械工業連合会，（社）日本電気計器工業会編，機械安全（電気装置）機能安全実用マニュアル”，初版(2001)，pp.100，日刊工業新聞社.
（23）ISO12100-2 : 2003, Safety of machinery-Basic concepts and general principles for design, Part 2：Technical principles(2003)，International Organization for Standardization.

第 5 章　空気圧駆動システムのインタロックによる安全確保と ISO13849 による安全関連系の整合性

5.1　はじめに

空気圧駆動システムにおける「安全」は，各種コンポーネント（結合部を含む）の強度設計とそれに基づく圧力制御を適切に行うだけでなく，過圧に対して安全弁等（減圧弁，リリーフ弁，ラプチャーディスクを含む）によって外気への放出を行う等，危険な圧力上昇を防ぐシステムを要求する．しかし，制御の誤りによる最大許容圧力を超える過負荷，また，それを回避するための安全弁等の故障（例えば弁の閉じ側の固着）の可能性が依然として解消されていない．例えば，空気圧駆動システムの圧力調整に広く使用されるレギュレータは，リリーフ弁の役目を兼ねており，そのため安全弁を要さないと考えるのが普通である．しかし現実には，レギュレータは弁の固着等による危険側故障が起こり得るが，そのためのインタロックが構成される例は殆どないと言っていい．また一方で，現状の空気圧駆動システムが，ALARP の原則による許容リスクの見方から，危険側故障に伴うリスクの評価を行って適正な手順に従った安全関連系の設計を行ったとする例もまた殆ど見当らない．

第 4 章において，空気圧駆動システムのインタロックシステム（以降，単に，インタロックシステム）の提案を行った．これは，駆動系に空気を供給する動力調整部の圧力に注目し，“窓監視”の方法で上昇側と下降側の両方の圧力を監視して危険側故障の影響を動力源遮断によって阻止するインタロックシステムの提案であった．しかし，本システムは，安全の妥当性の根拠を安全（確認）の原理 [(1)] に置いており，そのため，リスクベースとする制御に関わる安全規格（例えばISO13849）に必ずしも整合していない．これらの違いは，「安全」の根拠を，前者では「危険（故障を含む）→動力源遮断」，すなわちフェールセーフとするのに対して，後者はリスク低減手段（安全関連系）の危険側故障の発生確率に置いていることで生じていると考えられる．

そこで，本章では，改めて，インタロックシステムと国際規格で規定される安全関連系との整合性について検討を行う．そのため，第 5.2 節では，本研究で提案するインタロックシステムの安全コンセプトを明らかにし，安全（確認）の原理に根拠を置く安全確保の妥当性について述べる．次に第 5.3 節ではインタロックシステムの機能および構

成条件について，第 5.4 節ではインタロックシステムを，機械安全に関する国際規格 ISO12100-1，2 と制御安全に関する国際規格 ISO13849-1 の見方からの検討を行い，このインタロックシステムの国際規格との整合性について考察する．

第 5.5 節では，インタロックシステムについて ISO13849-1 で規定される安全関連系としての評価を行う．インタロックシステムは，遮断弁を用いて，故障時，空気圧駆動システムから切り離す構成である．これにより，空気圧コンポーネントの危険側故障はすべて，インタロックシステムの遮断構造に集約されると見ることができる．さらにフェールセーフな“窓監視”と故障時の遮断弁の“OFF 遮断”を採用することによって，危険側故障の影響を生じない理想的な安全関連系であることが期待される．本章で，これらの検討によって上記 2 つの安全の妥当性が整合可能であることを示そうとするものである．

5.2 インタロックシステムにおける安全コンセプト

リスクを基調とする国際規格ISO12100 やISO13849 は，“使用の制限”，“意図する使用”，“合理的に予見可能な誤使用”に伴う「事故（危害）」の可能性をリスクで表し，機械やシステムの運転実行に当って，社会的に容認されるレベル（許容リスクレベル）を達成すべきと規定する．しかし，現実には，そのレベルを達成できない場合が起こり得る．特に，リスク低減のために導入した手段が故障でリスクを増大させる場合が問題とされる．このような故障を危険側故障と言うが，国際規格は，実用上，許容リスクレベルの代わりに，リスク低減のための手段（安全関連系）の危険側故障の発生確率を許容レベルに抑えることを要求している．これに対して，本章で提案するシステムは，安全（確認）の原理 [(1)] に準拠し，危害の可能性を有する機械的出力が「安全」を許可条件とする構成であり，安全が確認できないとき（危険を含む）許可の停止とともに負荷出力を遮断する．このとき誤って危険な負荷を生じさせる故障が危険側故障である．本システムは，故障による危険な負荷を発生する確率を小さくするという考え方でなく，図 4.5 に示すようにインタロックシステムを構成し，故障で安全が確認できないとき動力を遮断することによって，危険側故障そのものの発生を防止することを安全のコンセプトとする．

すでにインタロックシステムの論理的構成法について実機に近いモデル（13 種類）を用いて報告 [(2)] したが，それは，空気圧コンポーネントの故障による危害防止のためのインタロックシステムの故障を安全側とするための提案であった．これは，基本的に，安全確保のシステムである限り，故障を，単に安全側とするのでなく，危険側故障の可能性に対して動力遮断による負荷の停止を達成すべきとする主張に基づくもので，これを実現したインタロックシステムは，危険側故障の影響を与えない理想的な安全関連系と認められてしかるべきである．これが，国際規格ISO13849 に対する本論文における

安全コンセプトの立場である．このように，2 つの見方から安全の妥当性が論じられている現状において，これらの整合化が可能か否かを検討することが本論文の趣旨でもある．

上記のコンセプトに基づき，図 3.1 のモデルを構成する 13 種の空気圧コンポーネントについて行った FMEA（Failure Mode and Effects Analysis）に再度注目する．分析の詳細については第 3 章にゆずることする．（結果の一部を表 3.6 に示してある）図 3.1 について改めて確認すれば, FMEA では故障モードの影響を P1, P0 について評価している．P1 の位置は動力調整部の出力であり，P0 はシリンダの動作により圧力変動が大きい位置である. そのため, 故障モードにより危険側故障が発生する可能性が高い部分である．FMEA は空気圧コンポーネントの故障モードが P1，P0 で発生する危険側故障の抽出を目的として行ったものである．その結果，故障モードは 220 件に上り，そのうち 15 件は圧力が上昇する側の故障モード（すなわち危険側故障），140 件は圧力が低下する側の故障モード，残りの 65 件が圧力の変化に影響しない故障モードであった．少数であるが, 明らかにコンポーネントに危険側故障が存在することが示された. 表 3.6 の FMEA の結果で示されるように，インタロックシステムは空気圧コンポーネントで P1，P0 を上昇させる故障モード（危険側故障）の影響を防ぐことを目的として構成される．

5.3 インタロックシステムの機能

5.3.1 機能の構成

第 5.2 節に示しているように，インタロックシステムは最初に提示した安全コンセプトを，満たすことで達成するとともに，当初の目的である危険側故障の影響を本質的に回避すると言う条件で，空気圧駆動システムの制御の安全を実現している．改めて，安全コンセプトに関する安全機能についてまとめると次の通りである．

空気圧駆動システムではレギュレータのP1 の初期設定，異常停止の原因の措置と再起動，修理・保全など，人手作業が存在する．特に，Q0=0 によるOFF遮断後の再起動は，異常の原因を排除した後，人の操作によってQ1=0 からQ1=1 の窓の条件に持っていく必要がある．この操作を可能とするために強制的にQ0=1 を作り出すためのホールド・ツーラン構造のスイッチ [(3)] が準備される．非定常の人手作業は別途検討を要するが，あくまでも，人間は，安全機能を担うのでなく安全機能の条件を管理する立場である．再起動における圧力P1 の再設定は，その範囲が，設計で規定された安全範囲がセンサスリットによるQ1=1（窓）固定しているため，人間の設定における危険側誤りの可能性は解消されている．

5.3.2 窓監視機能

“窓監視”はシステムの運転中における圧力の挙動を監視する機能である．動力調整部

P1 の圧力の上限と下限にしきい値を設けて，そのしきい値の内側にあることを運転許可の条件としている．センサによる監視は，常時なされており，また，ウインドゥ・コンパレータ (4) ~ (8) は 50KHzの交流処理を行ってセンサの故障をチェックしている．したがって，センサによる安全確認は常時実行されていると見ていい．

5.3.3 調整機能

“窓監視”によって圧力が窓の外側を示した場合，Q0=0 となって P1 は遮断・放出されるが，センサの故障，ウインドゥ・コンパレータの故障などを Q1=1（危険）と見なして Q0=0 が運転に介入して遮断弁により動力源遮断が実行される．さらに，遮断操作は受動的に行われるため，遮断弁自体が，例えば供給する電流が断線しても，遮断弁の遮断が実行される．

5.3.4 停止機能

窓もともと，誤りのない圧力の設定と，リリーフ機能（安全弁としての機能）をもつレギュレータが完全であれば，安全のために遮断機能を持つ必要はないと言える．空気圧，特に高圧の空気圧は大きな被害の潜在性を有する危険源であり，安全の要求に対して，危険側故障やミスが存在するレギュレータや人間が応えるのは本来不可能である．

本論文では，危険の発生は「停止」に置き換えられるため，レギュレータや人間は解放されて，安全側か危険側かとは無関係に，圧力調整の本来的機能の性能／信頼性等（パフォーマンス）の高度化を指向できる．安全性（フェールセーフ）を信頼性と独立して確保すれば，機能の高度化への指向が可能となる．

5.4 国際規格による評価

5.4.1 関連する国際規格

インタロックシステムに関係する国際規格は主に次の 3 つが該当し，これによりインタロックの構成法および機能について関連性と相違点について検討する．

（ⅰ）ISO12100-1（機械類の安全性－設計のための基本概念，一般原則－第 1 部：基本用語，方法論） (9)

（ⅱ）ISO12100-2（機械類の安全性－設計のための基本概念，一般原則－第 2 部：技術原則） (10)

（ⅲ）ISO13849-1（制御システムの安全関連部－設計のための一般原則） (11)

5.4.2 ISO12100-1，2 による評価

安全機能とは，危険を予測して事故を防ぐ機能，あるいはそれに関連してリスクを下げる機能と言うことができる．ISO12100-2 によれば，概ね，故障するとリスクが増大する機能とされる．そして，安全関連系とは，安全機能を実行するハードウェアと理解される．インタロックシステムは，安全機能を実行する明らかに安全関連系と認められる．しかし，インタロックシステムにおける安全の立場は，リスク低減機能を安全機能とはしていない点に注意が必要である．本論において「事故を防ぐ」とは，事故が生ずる前に危険な行為を停止することだと定める．

ISO12100 では，安全の対象を人間が被る危害においている．したがって，対象とするシステムや機械が人間とどう関わるかによってリスク評価が大きく変わってくる．空気圧駆動システムは医療機器などの人間と密接な関係で使用される場合から自動化ラインなど人間と離れて使用される場合まで使用環境が幅広い．設計での想定（意図する使用）とは異なる使用がなされることも大いにあり得る．そのため，インタロックシステムは使用とは関係なく動力源遮断することで無条件に安全確保できる立場に立ち，ISO12100-1 の 5.2 項「機械の制限に関する仕様」の“使用上の制限”，“空間上の制限”に安全の特別の条件を要求しない．

インタロックシステムは，人間の調整操作，機器による調整機能，安全の確認，危険時の遮断と言う安全の基本を実行するばかりでなく，安全機能自体（安全関連系）に故障が生じたとき遮断によってリスク発生を阻止しており，そのため ISO12100-1 の 3.19「本質安全設計方策」の要求に応える保護方策であると評価されてしかるべきである．

ISO12100-2 の 4.11「制御システムへの本質的安全設計方策」では，制御システムの設計方策は，安全関連性能が十分リスク低減ができるように選択されなければならないと規定される．インタロックシステムは窓監視によって危険な故障を検知して動力源遮断を行い，危害防止の要求に応える構成をとっている．

具体的には，インタロックシステムで圧力の上限と下限のしきい値による窓監視は 4.11.6「自動監視の使用」の要求に，また遮断弁による動力源遮断と同時に行われる排気は 4.11.5「動力供給の中断」と 5.5.4「遮断及びエネルギーの消散に関する方策」の要求に適合している．

図 4.2 の窓監視用のセンサ，ウインドゥ・コンパレータは非対称故障モード特性を有しており，遮断弁はノーマルクローズタイプ [(12)] を使用している．したがって，センサ，ウインドゥ・コンパレータ，遮断弁は 4.12.2「非対称故障モードの構成品の使用」に適合している．

インタロックシステムは ISO12100-1，2 の要求に応え，基本的には規格の要求に準拠している．さらに，空気圧駆動システムの圧力制御に伴う危険側誤りに対して動力源遮断により「危害」を防ぐことにより，リスクの生成を防止することを目指した本質安全設計方策を実現した実用的なシステムであると評価されてしかるべきである．

5.4.3 ISO13849-1 による評価

ISO13849-1 はタイプ B 規格であるため, ISO12100-1,2 の要求事項が引用されている. ここでは, 前項で評価を行った ISO12100-2 の 5.5.4 項による評価も含まれる. ISO13849-1 は制御システムの安全関連部（系）における設計のための原則を示している．制御システムの安全関連部（以下，安全関連部とする）とは 3.1.1「安全関連入力信号に応答し，安全関連出力信号を生成する制御の部分」と規定されている．安全関連部の設計では安全性の目標，リスク低減については ISO12100-1，2 の要求に準拠し，またインタロックシステムは ISO12100-2 の 6.2 項でに準拠すると述べている．

インタロックシステムによって行われる窓監視，動力遮断による停止，動力遮断と同時に行われる排気は 5「安全機能」の監視，非常停止機能，遮断及びエネルギーの消散に該当する．窓監視のセンサから出力される電圧とウインドゥ・コンパレータから出力される交流信号がそれぞれ，3.1.1 の安全関連部の定義に規定されている安全関連入力信号，安全関連出力信号に該当する．

ISO13849-1 では安全関連部と非安全関連部は分離して，非安全関連部の制御出力は安全関連部の許可がなければ出力できないインタロックで構成することが規定されている．このことは，インタロック構成上の基本であって，インタロックシステムでは窓監視により「安全」と判断されたときのみ動力供給が実行され，窓外にあって「危険」と判断されたときは空気圧駆動システムの動力源は遮断される．また，窓監視の故障は Q0=0 によってまた遮断弁の故障も遮断弁の OFF 遮断につながっていて，すべて故障は遮断弁の OFF 遮断につながっているという意味で，相互に異常は独立していると見ることができる．このように，インタロックシステムは，図 4.1 に示すように，危険の発生によって，遮断弁の OFF 遮断によって空気圧駆動システムとは切り離される構成である．インタロックシステムは，残留リスクを容易に認めないとする厳格さの点では異なるが，基本的には，ISO13849-1 の要求に準拠し構成されている安全関連系であると見ることはできる．

安全関連部の評価は ISO13849-1 の 6「カテゴリと各チャネルの MTTFd（危険側故障発生確率），DCavg（平均診断範囲）及び CCF（共通原因故障）の関係」では特定の PL（パフォーマンスレベル）を達成するための基本的なパラメータであるカテゴリで評価することを要求している．カテゴリは B～4 までの 5 段階の評価で MTTFd の低さで評価されている．インタロックシステムを構成する遮断弁，センサ，ウインドゥ・コンパレータは故障が発生しても危険側故障にならない非対称故障モードの特性を有している．そのため，カテゴリ評価を行ってみると危険側故障の発生自体を限りなく抑制しているためカテゴリ 4 以上の評価が可能である．また, 窓監視によりセンサ, ウインドゥ・コンパレータの正常性確認を行っているためこれらの故障による誤判断の危険側故障の発生を限りなく抑制している．さらに，インタロックシステムは危険側誤りに対して動力を遮断しており, 危険側故障の発生自体を抑制しているためカテゴリ評価の枠を超

えて普遍的な安全を指向していると言っていい.

インタロックシステム全体としては ISO12100-1,2 および ISO13849-1 の要求に応え，規格に示された手順により構成されている実用的な安全関連部であると評価することができる.

5.5 安全関連部（系）としてのインタロックシステム

安全確認システムは，安全（確認）の原理に基づき，予め事故（危害）が生じないことを確かめて危険を伴う制御行為を実行するとするインタロックシステムである. 前提として重要なことは，まず，確認すれば安全だと言える「安全」が明確に規定されること，もう一つは，それが確認できなければ停止して事故を防ぐための停止手段が存在することである. それをなしに実行される安全機能は不完全であるためリスクを生ずるが，その不完全性に対するリスク評価を行って許容しようとするのがリスクベースの安全と言うことができる.

インタロックシステムは，第 5.4 節における検討によって ISO12100 や ISO13849-1 で規定される安全関連部（系）に基本的に準拠すると認められるが，それだけであれば，許容リスクレベルを達成するためのリスク低減方策と何ら変わりない．人間が「安全」に関わるとき，もともと安全な機械やシステムとして与えられるわけでなく，危険を伴う操作を安全に行って事故（危害）を防いでいるのである．安全（確認）の原理において確認されるべき「安全」とは，安全に使用する条件（設計者の意図する使用と使用の制限）として設計者によって規定され，使用者はそれに準拠して安全に使用すると言う関係である．ここに改めて，安全に作業ができないとき作業を停止して事故を防ぐことが重要であるが，この構成が，いつでも停止できる条件で危険な作業が実行されているとするインタロックとして理解する必要がある．リスク発生は，作業を停止すべきとき停止しない，あるいは停止が遅れて生ずるとする危険側故障で発生する．したがって，安全が確認できないとき作業を強制停止するシステムを実現しない限りリスク発生を防止することはできないと言える.

ISO12100 と ISO13849 における国際規格の考え方は，安全関連部における「安全」が何によっているのかが明確でない．したがって，安全が確認できないとき事故の前で停止すべきとする厳格な停止の条件が規定されていない．追及に曖昧さを含む本質から，「安全」は確率的事象（リスクベース）とせざるを得ず，そのため致命的と言えるような大きな被害を伴う事故への適用には明らかに限界がある. このような事故の発生は確率論に委ねることができないからである.

インタロックシステムは，決定論（確定論）[13] に基づく．安全を確認して危険の可能性のある機械的制御の実行を許可するとするシステム（安全機能）を実行するハードウェア（安全関連部）であり，インタロックシステムは，リスク発生の要因である危険

側故障の影響を動力源遮断で防いでいる.

ISO13849-1 は，安全関連部と非関安全連部を別に扱うよう求めているが [14]，図 5.1 では, 安全確認を受ける側を非安全関連部, 安全確認を実行する側を安全関連部として, 両者がインタロックの関係で関連づけられている [15]．図 4.7 のインタロックと図 5.1 を比較して分かるように，安全関連部としてのインタロックシステムは，設計者によって規定される安全をユネイトな論理的関係で実行する安全確認機能（Q1≧Q0）と正当な構造を持つ遮断構造（P1*）からなり，フェールセーフなウィンドウ・コンパレータの窓監視によって，レギュレータ等空気圧コンポーネントの危険側故障の影響を解消していると結論される.

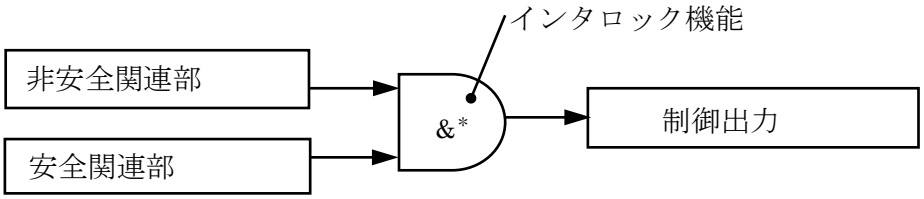


図 5.1　制御システムにおける安全関連部と非安全関連部の関係 [15]
（安全関連部と非安全関連部とは相互に独立することが基礎的条件）

5.6　小括

本論文ではインタロックシステムと国際規格で規定される安全関連系との整合性について検討を行った．インタロックシステムの安全コンセプトを明らかにし，安全（確認）の原理に根拠を置く安全確保の妥当性について述べている.

インタロックシステムの安全コンセプトはシステムを構成するコンポーネントの故障，インタロックシステム自体の故障による危害の防止である.

インタロックシステムについて機械安全に関する国際規格 IS12100 と制御安全に関する国際規格 ISO13849-1 の見方からの検討を行い，国際規格との整合性について考察を行った.

ISO12100 による見方での検討では基本的には規格の要求に準拠しており本質安全設計方策を実現した実用的なシステムであると評価できる．また，ISO13849-1 ではインタロックシステムは危険側誤りに対して動力を遮断しており, 危険側故障の発生自体を抑制しているためカテゴリ評価の枠を超えて普遍的な安全を指向していると言っていい．したがって，インタロックシステム全体としては ISO12100 および ISO13849-1 の要求に応え, 規格に示された手順により構成されている実用的な安全関連部であると評価することができる.

しかし，ISO12100とISO13849-1における国際規格の考え方は，安全関連部における「安

全」が何によっているのかが明確でなく，安全が確認できないとき事故の前で停止すべきとする厳格な停止の条件が規定されていない問題点がある．インタロックシステムは，決定論（確定論）に基づく．安全を確認して危険の可能性のある機械的制御の実行を許可するとするシステム（安全機能）を実行するハードウェア（安全関連部）であり，インタロックシステムは，リスク発生の要因である危険側故障の影響を動力源遮断で防ぐ実用的なシステムと言える．また，リスク低減とする代わりに危険時の緊急停止によってリスク発生を防ぐとする点で，リスクベースの国際規格とは異なるが，緊急時の停止が実質的にリスク低減をもたらすと考えれば，安全（確認）の原理が志向する安全とリスクベースの安全とは本質的には同じとみて矛盾はない．

第 5 章　参考文献

（1） 杉本旭, 蓬原弘一“安全の原理”, 日本機械学会論文集 C 編, Vol.56, No.530(1990), pp.75-83.

（2） 中村瑞穂, 田中慎也，杉本旭，“空気圧駆動システムにおける危険側故障を解消するためのインタロックの提案”, 日本機械学会論文集 C 編，Vol.79, No.805(2013-9)， pp.167-177.

（3） 労働省安全衛生部安全課監修，“これからの安全技術－工作機械等の制御機構のフェールセーフ化に関するガイドラインの解説”，中央労働災害防止協会，2000 年 1 月，pp.62.

（4） 蓬原弘一，向殿政男，“窓特性をもつフェイルセーフ論理素子を使ったインタロックシステムの－構成法”，電気学会論文集 C 編，Vol.109，No.9（1989），pp.676-683.

（5） 蓬原弘一，杉本旭，向殿政男，“フェールセーフ・ウィンドゥ・コンパレータの構造とその応用”，第 18 回 FTC 研究会資料.

（6） 蓬原弘一，“非対称誤り素子によるフェイルセイフ論理回路の一構成法”，電気学会論文集 D 編，Vol.104，No.2(1984)，pp.29-34.

（7） *Futsuhara,K.,Sugimoto,N.,andMukaidono,M.,“Fail-Safe Logic Elements Having Upper and Lower Thresholds and Their Application to Safety Control”, Digest of Papers of FTCS-18,Poster Session(1988-6,Tokyo).*

（8） (社) 日本労働安全衛生コンサルタント会編, これからの安全技術, 第 1 版（2000），pp.81-82，中央労働災害防止協会.

（9） ISO12100-1:2003,Safety of machinery-Basic concepts and general principles for design, Part 1 : Basic terminology，methodology(2003)，International Organization for Standar dization.

（10） ISO12100-2：2003，Safety of machinery-Basic concepts and general principles for design，Part 2：Technical principles(2003)，International Organization for Standar dization.

（11） ISO13849-1:2006，Safety of machinery-Safety-related parts of control systems, Part1:General principles for design(2006)，International Organization for Standar dization.

（12） 蓬原弘一著，“安全工学基礎ノート”，2000 年 8 月，長岡技術科学大学，pp.39

（13） 杉本旭，“確率論と確定論に基づく安全の構成”，信頼性学会誌

（14） 白井稔人，坂井正善，蓬原弘一，“安全関連部と非安全関連部の分離に基づく安全制御システムの - 実現方法”，信学技法，1999．pp.7-10.

（15） 蓬原弘一編著，“安全コンポーネントの構成原理とその適用”，2010 年改訂版，pp.34-35，安全応用研究会.

第 6 章　総括

本論文では，空気圧システムの構成例を示し，これを構成するコンポーネントについて FMEA を適用して故障モードの検討を行った．その結果，いくつかのコンポーネントで圧力が上昇する危険側の故障モードの存在が明らかとなった．また，低下する側の故障モードも多く存在するため，空気圧システムの故障監視には，圧力の上昇と低下の両方を監視するのが有効である．

安全の共通の原理に準拠したフェールセーフ・システムはユネイトな論理的関係で実現されるとされている．そこで，空気圧システムの構成例を①動力供給部，②動力調整部，③駆動系に分離し，動力調整部に注目し駆動系との分離点における動力調整部圧力に対し上昇／低下を監視する窓監視を提案している．

窓監視によるインタロックを構成するため，本論文では窓監視を可能とするセンサを開発し，これに ISO13849-1 による安全要求を満たすウインドゥ・コンパレータを適用して，ユネイトな論理的関係を条件とするフェールセーフ・インタロックの実現可能性を示した．また，フェールセーフは非対称故障モードによって実現されるとする ISO12100-1 の見方から改めて検討を加え，本システムがこの立場からもフェールセーフに矛盾していないことを明らかにした．フェールセーフ・インタロックの重要な条件である動力遮断の故障特性に関し，窓監視によるフェールセーフ・インタロックに備えるべき遮断構造について検討を行なった．

本論文の FMEA による故障モードは ISO13849-2 の付属書 B（空気圧システムの妥当性確認ツール）に本質的に矛盾するものでなく，安全（確認）の原理に従って検討を行った結果，本システムは，機械安全の国際規格 ISO12100-2 にほぼ準拠していると言える．さらに機械の制御安全の国際規格 ISO13849-1 では安全関連部の危険側故障の発生確率の低減が要求されている．本システムでは危険側誤りに対して動力を遮断しており，危険側故障の発生自体を抑制していると言える．

このインタロックシステムと国際規格で規定される安全関連系との整合性について検討を行った．インタロックシステムの安全コンセプトを明らかにし，安全（確認）の原理に根拠を置く安全確保の妥当性について述べ，安全コンセプトはインタロックシステムの故障を，危険側だけなく安全側を含めて監視し，システムを構成するコンポーネント（センサ，ウインドゥ・コンパレータ，遮断弁）の故障，インタロックシステム自体の故障による事故（危害）の防止である．

インタロックシステムは窓監視により圧力制御に伴う危険側誤り，インタロックシステム自体の故障に対して動力源遮断により危険側故障によるリスク発生を解消するシステムであると言える．

このインタロックシステムについて機械安全に関する国際規格 IS12100-1，2 と制御安全に関する国際規格 ISO13849-1 の見方からの検討を行い，国際規格との整合性について考察を行った結果，ISO12100-1，2 では基本的には規格の要求に準拠しており本質安全設計方策を実現した実用的なシステムであると評価できる．また，ISO13849-1 ではインタロックシステムは危険側誤りに対して動力を遮断しており，危険側故障の発生自体を抑制しているためカテゴリ評価の枠を超えて普遍的な安全を指向していると言っていい．したがって，インタロックシステム全体としては ISO12100 および ISO13849-1 の要求に応え，規格に示された手順により構成されている実用的な安全関連部（系）であると評価することができる．

しかし，ISO12100とISO13849における国際規格の考え方は，安全関連部における「安全」が何によっているのかが明確でなく，安全が確認できないとき事故の前で停止すべきとする厳格な停止の条件が規定されていない問題点がある．インタロックシステムは，決定論（確定論）に基づく．安全を確認して危険の可能性のある機械的制御の実行を許可するとするシステム（安全機能）を実行するハードウェア（安全関連部）であり，インタロックシステムは，リスク発生の要因である危険側故障の影響を動力源遮断で防ぐことから実用的で理想的なシステムであり安全（確認）の原理が志向する安全とリスクベースの安全とは本質的には同じとみて矛盾はない．さらに，安全（確認）の原理における構成法が国際規格に基づく構成法よりも優れた安全関連系の構成が可能であると言える．

本研究において，提案したインタロックシステムは窓監視と動力遮断により危険側故障の影響を防ぐことが可能である決定論（確定論）に基づく安全システムを提案したが，既に規格で規定されている空気圧システムに関する安全（例えばアクチュエータの危険動作など）と組み合わせて活用することと，また，インタロックシステムの構成と構成プロセスを他のシステムへ応用することにより実用的な安全システムの構成に適用する．さらに，インタロックシステム自体が国際規格に準じており実用的で理想的なシステムであるため空気圧システムの安全および国際安全規格の教育訓練への教材として適用することが今後の課題である．

謝辞

本研究を進めるにあたり，指導教員である明治大学理工学部理工学研究科新領域創造専攻安全系　杉本旭教授には 7 年間という長きにわたり，理論的な研究の進め方，論文の作成方法, 査読論文の照会への対応など懇切丁寧なご指導を賜りましたことに心から深く感謝いたします.

本研究を学位論文にまとめるにあたり, 副査としてあたたかいご指導とご教示をいただいた明治大学理工学部大学院理工学研究科新領域創造専攻安全系　山本俊哉教授（系長)，向殿政男名誉教授に深甚なる謝意を表します.

また，明治大学理工学部システム安全研究室（杉本研究室）の田中慎也氏，芳司俊郎氏，戸枝毅氏を始めとする諸氏の熱心な協力を頂き厚く御礼申し上げます.

そして，長岡技術科学大学大学院工学研究科機械創造専攻博士課程前期社会人キャリアアップコース機械安全工学在籍中には，私が安全工学を初めて学ぶにあたり懇切丁寧にご指導, ご鞭撻を賜りました長岡技術科学大学　蓬原弘一名誉教授には心から感謝申し上げます．さらに，博士論文説明会を始め学会等で本研究について貴重なご意見，ご鞭撻を賜りました長岡技術科学大学大学院　福田隆文教授に厚く御礼を申し上げます.

本研究において FMEA のご指導，ご助言を頂きました元日立製作所日立工場原子力予防保全センター長の小野寺勝重氏に厚く御礼を申し上げます.

明治大学大学院に通学にあたりご配慮および激励を頂きました職業能力開発総合大学校ならびに東京校の古川勇二校長，谷中善典副校長，田中敏博副校長，坪内茂樹前副校長（現，高度職業能力開発促進センター所長)，原寛志管理部長，荒隆裕教務部長，中村佳史元教授，千葉正伸教授，前田晃穂教授，笹川宏之准教授，市川修准教授，南川秀樹特任准教授，安原雅彦准教授，菊池拓男助教，太田和良助教，新家寿健特任助教，鳥濱博氏ならびに職業能力開発総合大大学校の教職員諸氏厚く御礼を申し上げます.

長岡技術科学大学大学院に通学する際にご配慮，応援，激励を賜りました群馬職業能力開発促進センター　神尾実元所長，同　山口穣元所長，　同　安部武元所長ならびに同職員諸氏の多大なるご協力を頂きました．厚く御礼を申し上げます.

茨城大学工学部システム工学科に通学する際にはご配慮，応援，激励を賜りました片寄益己氏他，三和工機株式会社の諸氏，日立製作所日立工場火力設計部タービン計画の諸氏，卒業研究等のご指導を賜り，卒業後も本研究を進めるにあたり激励を賜りました茨城大学システム工学科　江田弘名誉教授，同　周立浪教授，同　清水淳教授につきま

しては心より感謝申し上げます.

関東職業能力開発大学校生産機械システム技術科　伊藤昌樹能開教授には茨城職業能力開発短期大学校生産技術科の在学中から現在に至るまで, 公私ともに数多くの貴重なご指導，ご鞭撻，激励を賜り，筆者が研究に興味を持ちだしたのも伊藤能開教授との出会いが無ければ有り得なかったことから心より深く感謝申し上げます.

本研究により学位論文を作成することができたのは茨城職業能力開発短期大学校, 三和工機株式会社，日立製作所日立工場火力設計部タービン計画，茨城大学，雇用・能力開発機構　福島職業能力開発促進センター，群馬職業能力開発促進センター，長岡技術科学大学，職業能力開発総合大学校（東京校)，明治大学と企業，大学，職業能力開発施設などで勤務, 学ぶことにより様々な人々との出会いと出会った人たちからのご指導, ご鞭撻，ご支援，ご協力によって完成することができ，ここにお名前を記すことが出来なかった多くの方々も含めて心より感謝申し上げます.

最後になりますが，私が理工系の道に進み学士，修士，博士を取得することを喜び, 期待してくれていた平成 10 年 10 月 23 日に永眠した父にこの論文を捧げるとともに, 長きにわたり私を応援してくれた母, 兄, 義姉と友人と家族に心より感謝申し上げます.

本研究の一部を発表した研究論文および口頭講演

1.学会誌等論文（査読有り）

（1） 中村瑞穂，田中慎也，杉本旭：空気圧駆動システムにおける危険側故障を解消するインタロックの提案，日本機械学会論文集（C 編 ， Vol.79,No.80（2013-9）,pp.167-177.（第 2,3,4 章）

（2） Mizuho Nakamura，Shinya Tanaka，Noboru Sugimoto：Proposal of Interlock System in Pneumatic and Hydraulic Control Systems，5th International Conference Safety of Industrial Automated Systems（Presentation）, pp.251-256 International Conference Safety of Industrial Automated System.（第 2,3,4 章）

（3）田中慎也，中村瑞穂，杉本旭：空気圧駆動システムに適用されるインタロックシステムの安全関連部(ISO13849)としての妥当性確認, 日本機械学会論文集（C 編 ，査読中.（第 5 章）

2.著書

（1）中村瑞穂，笹川宏之，古井英則：「PLC（プログラマブルロジックコントローラ）によるメカトロ制御入門」（本人担当部分:第 7 章 PLC による空気圧制御 pp147-169）

3.口頭講演

（1）中村瑞穂，田中慎也，杉本旭：安全制御の原理による圧力容器の安全システムの考察，日本機械学会 2013 年度年次大会（2013.09.10 岡山大学津山キャンパス）

（2）中村瑞穂，田中慎也，杉本旭：空気圧駆動システムの危険側故障を解消するインタロックの提案，安全工学シンポジュウム 2013（2013.07.04 東京都，日本学術会議）pp.348-351

（3）中村瑞穂，田中慎也，杉本旭：空気圧駆動システムの圧力制御における危険側誤りを解消するインタロックの提案，日本機械学会　産業・化学機械と安全部門講演論文集 2013（2013.06.21 横浜国立大学）pp.19-20.

（4）中村瑞穂，千葉正伸，杉本旭：空気圧駆動システムにおける安全関連部の構成論

理とインタロックの提案, 第 21 会日本信頼性学会春季シンポジュウム（2013.06.12 東京都，日科技連）pp.35-38.
（5）中村瑞穂，田中慎也，杉本旭：安全制御の原理による圧力容器の安全システムの考察，第 45 回安全工学研究発表会（2012.11.29 東京都，女性就業支援センター）pp.97-100.
（6）中村瑞穂，田中慎也，杉本旭：自動車の運転と安全確認システムにおけるアクティブ・セーフティーの役割，安全工学シンポジュウム 2012（2012.11.29 日本学術会議）pp.392-393.
（7）中村瑞穂，田中慎也，杉本旭：安全制御の原理，第 44 回安全工学研究発表会（2012.12.02 山形県，伝国の杜）pp.215-218.
（8）中村瑞穂，杉本旭：品質としての「安全」とは区別すべき安全性の妥当性確認について，2010 年度　産業・化学機械と安全部門講演論文集（2010.11.25 東京工業大学，大岡山キャン）pp.9-10.
（9）中村瑞穂，杉本旭：EN764-7 に基づく油空圧制御システムの安全確認システム，第 18 回春季信頼性シンポジュウム（2010.05.28 東京都，日科技連）pp.65-68.
（10）中村瑞穂，蓬原弘一：空気圧制御システムの論理的構造とその適用，第 19 回秋季信頼性シンポジュウム（2006.10.20 東京都，日科技連）pp.73-76

付録 A　空気圧機器の FMEA

付表 1　コンプレッサの FMEA(1/9)

部品名	故障モード	論理値	挙動		
			Pg コンプレッサ出力	P1 方向制御弁入力	P0 シリンダ出力
吸込弁	開放	1	影響なし.	影響なし.	影響なし.
	閉止	0	空気を吸入できないため Pg は出力せず.	圧縮空気が供給されないので P1 は出力しない.	圧縮空気が供給されないので P0 は出力しない.
	詰まり	0	空気を吸入できないため Pg は出力せず.		
	外部リーク	0	吸入した空気が漏れ，Pg は出力せず.		
		1	吸入した空気が漏れるが Pg には影響がない.	影響なし.	影響なし.
	内部リーク	0	吸入した空気が漏れ，Pg は出力せず.	圧縮空気が供給されないので P1 は出力しない.	圧縮空気が供給されないので P0 は出力しない.
		1	吸入した空気が漏れるが Pg には影響がない.	影響なし.	影響なし.
吸込フィルタ	目詰まり	1	目詰まり量が少ないため空気を吸入できる．Pg には影響はない.		
		φ	目詰まり完全ではないため空気を吸入できるが圧縮空気の排出量に影響がでる.	圧縮空気の量が少ない.	P0 の動作が鈍くなる.
		0	完全に目詰まりしているので空気を吸入できないため Pg は出力されない.	圧縮空気が供給されないので P1 は出力しない.	圧縮空気が供給されないので P0 は出力しない.
	破損	1	空気を吸入することができるが清浄度に問題がある.	影響なし.	影響なし.
		φ	空気を吸入することができるがやがては機器に影響がでて圧縮空気の排出量に影響がでる.	圧縮空気の量が少ない.	P0 の動作が鈍くなる.

付表 1　コンプレッサの FMEA(2/9)

部品名	故障モード	論理値	挙動		
			Pg コンプレッサ出力	P1 方向制御弁入力	P0　シリンダ出力
吸込フィルタ	破損	0	塵埃，湿度により機器が故障したため，Pg は出力されない.	圧縮空気が供給されないので P1 は出力しない.	圧縮空気が供給されないので P0 は出力しない.
シリンダ	破壊	0	空気が漏れピストンも動作しなくなるので圧縮空気は作られず Pg は出力されず.		
	亀裂	1	亀裂の大きさが小さいため亀裂部から空気が漏れるが影響はない.	影響なし.	影響なし.
		φ	亀裂の大きさが空気漏れを発生させる程度であるため，圧縮空気排出量に影響がある.	圧縮空気の量が少ない.	P0 の動作が鈍くなる.
ピストン	固着	0	ピストンがシリンダ内面に固着して動作しなくなるので Pg は出力されず.	圧縮空気が供給されないので P1 は出力しない.	圧縮空気が供給されないので P0 は出力しない.
	破壊	0	空気の圧縮工程が喪失されるので Pg は出力されず.		
	偏芯	1	偏芯の大きさが小さいのでピストンの動作には影響がない．従って，Pg は出力される.	影響なし.	影響なし.
		ϕ	偏芯の大きさが動作を鈍くしているので圧縮空気の排出量に影響がある.	圧縮空気の量が少ない.	P0 の動作が鈍くなる.
ピストンピン	固着	0	ピストンピンが固着してシリンダピストンが動作しなくなるので Pg は出力されず.	圧縮空気が供給されないので P1 は出力しない.	圧縮空気が供給されないので P0 は出力しない.
	破壊	0	ピストンピンが破壊してシリンダピストンが動作しなくなるので Pg は出力されず.		

付表 1　コンプレッサの FMEA(3/9)

部品名	故障モード	論理値	挙動		
			Pg コンプレッサ出力	P1 方向制御弁入力	P0 シリンダ出力
ピストンリング（圧力リング）	亀裂	1	亀裂の大きさが小さいのでピストンの動作には影響がない．従って，Pg は出力される．	影響なし．	影響なし．
		ϕ	亀裂の大きさが，空気が漏れる程度であるため圧縮空気の排出量に影響がある．	圧縮空気の量が少ない．	P0 の動作が鈍くなる．
	破壊	0	ピストンリングが破壊して空気が漏れるため圧縮空気が排出されず Pg は出力されない．	圧縮空気が供給されないので P1 は出力しない．	圧縮空気が供給されないので P0 は出力しない．
ピストンリング	亀裂	1	亀裂の大きさが小さいのでピストンの動作には影響がない．従って，Pg は出力される．	影響なし．	影響なし．
		ϕ	亀裂の大きさが，空気漏が起こる程度であるため圧縮空気の排出量に影響がある．	圧縮空気の量が少ないが，P1 は出力する．	P0 の動作が鈍くなる．
	破壊	0	ピストンリングが破壊して空気が漏れるため圧縮空気が排出されず Pg は出力されない．	圧縮空気が供給されないので P1 は出力しない．	圧縮空気が供給されないので P0 は出力しない．
連接棒	破壊	0	連接棒の破壊によりピストンが動作しなくなるので，圧縮空気が排出されないので，Pg は出力されない．	圧縮空気が供給されないので P1 は出力しない．	圧縮空気が供給されないので P0 は出力しない．
	亀裂	1	亀裂の大きさが小さいのでピストンの動作には影響がない．従って，Pg は出力される．	影響なし．	影響なし．

付表 1　コンプレッサの FMEA (4/9)

部品名	故障モード	論理値	挙動		
			Pg コンプレッサ出力	P1 方向制御弁入力	P0　シリンダ出力
連接棒	破壊	0	連接棒の破壊によりピストンが動作しなくなるので，圧縮空気が排出されないので，Pg は出力されない.	圧縮空気が供給されないので P1 は出力しない.	圧縮空気が供給されないので P0 は出力しない.
	亀裂	1	亀裂の大きさが小さいのでピストンの動作には影響がない．従って，Pg は出力される.	影響なし.	影響なし.
クランク軸	亀裂	1	亀裂の大きさが小さいのでピストンの動作には影響がない．従って，Pg は出力される.	影響なし.	影響なし.
	破壊	0	破壊により連接棒からピストンに動力が伝達されなくなるので，動作しなくなり，圧縮空気が排出されないので，Pg は出力されない.	圧縮空気が供給されないので P1 は出力しない.	圧縮空気が供給されないので P0 は出力しない.
	固着	0	軸受，連接棒，クランク軸受の各部のいずれかで固着が発生した場合，軸が回転しなくなるので連接棒から動力がピストンに伝達されなくなるので，圧縮空気が排出されないので，Pg は出力されない.		
クランク軸受 軸受け	振動大	0	軸受の交換や組立調整が必要であるため停止さる必要があるため，Pg は出力されない.		
	温度上昇	0	異常荷重，取付不良，潤滑油不足，過多，不適，摩擦が原因であるため軸受の交換や組立調整が必要であるため停止さる必要があるため，Pg は出力されない.		

付表 1　コンプレッサの FMEA (5/9)

部品名	故障モード	論理値	挙動		
			Pg コンプレッサ出力	P1 方向制御弁入力	P0 シリンダ出力
クランク軸受 軸受け	騒音	0	異常荷重，取付不良，潤滑油不足，過多，不適，摩擦,回転部品の接触，異物による傷，圧こん，隙間過大原因であるため軸受の交換や組立調整が必要であるため停止さる必要があるため，Pg は出力されない.	騒音.	
クランク軸受 軸受け	潤滑油の漏れ	0	潤滑剤の過多，異物侵入，摩耗粉の発生，侵入などにより，軸受の交換や組立調整が必要であるため停止させる必要があるため，Pg は出力されない.	圧縮空気が供給されないので P1 は出力しない.	圧縮空気が供給されないので P0 は出力しない.
軸受箱 （ハウジング）	はめあい部摩耗	0	摩耗粉が侵入して振動や異常な発熱の原因となることもあるので，組立調整が必要であるため，停止させる必要があるため，Pg は出力されない.		
	破壊	0	軸受けがカバーできなくなるので，停止させる必要があるため，Pg は出力されない.		
ベルト車	破壊	0	電動機からコンプレッサ本体に動力が伝達されなくなるので,Pg は出力されない.		
	ベルト溝の摩耗	0	ベルト車からベルトが外れ，電動機からコンプレッサ本体に動力が伝達されなくなるので,Pg は出力されない.		

付表 1　コンプレッサの FMEA (6/9)

部品名	故障モード	論理値	挙動		
			Pg コンプレッサ出力	P1 方向制御弁入力	P0　シリンダ出力
電動機	電源停止 モータ故障 容器の一部破壊 起動スイッチ故障 配線の断線 電圧降下 圧縮機の回転不良 リレー故障 ヒューズ切れ トランス故障 基盤故障	0	コンプレッサが動作しないため, 圧縮空気が供給されないので Pg は感知せず.		
ファン	破壊	1	コンプレッサの動作には影響がない. ＊冷却効果が無くなるので故障の原因となるので対策は必要である.	圧縮空気は供給され，P1 は出力する.	圧縮空気は供給され，P0 は出力する.
ファンカバー	破壊	1	コンプレッサの動作には影響がない. ＊カバーが破壊されたので回っているファンで怪我する可能性がある.	圧縮空気は供給され，P1 は出力する.	圧縮空気は供給され，P0 は出力する.
クランク室	破壊	0	コンプレッサが動作しないため, 圧縮空気が供給されないので Pg は感知せず.	圧縮空気が供給されないので P1 は出力しない.	圧縮空気が供給されないので P0 は出力しない.
	破損	1	破損箇所によっては, コンプレッサの動作には影響がない. 潤滑油漏れが起こりやがて故障を招く.	影響なし.	影響なし.

付表 1　コンプレッサの FMEA (7/9)

部品名	故障モード	論理値	挙動		
			Pg コンプレッサ出力	P1 方向制御弁入力	P0 シリンダ出力
クランク室	破損	ϕ	破損箇所によっては，コンプレッサの動作に影響があり，性能が低下する.	圧縮空気の量が少ないが P1 は出力する.	P0 が要求性能通り動作しない.
		0	軸受け部などが破損した場合，ベルト車の回転を停止させるので，動力が伝達されないので圧縮空気が供給されないので Pg は感知せず.	圧縮空気が供給されないので P1 は出力しない.	圧縮空気が供給されないので P0 は出力しない.
注油口	詰まり	ϕ	給油ができなくなり，機器の損傷，故障を招く.	圧縮空気は供給され，P1 は出力する．故障・損傷が発生したら出力しない.	圧縮空気は供給され，P0 は出力する. 故障・損傷が発生したら出力しない.
	破壊	ϕ			
	開かない	ϕ			
	閉じない	ϕ	潤滑油の中に塵埃，水分，他物質が入り故障の原因を作り出す.		
油面計	破壊	ϕ	潤滑油の入っている量が分からず，注入時期などを忘れる可能性があり，怠ると故障，損傷の原因となる.		
油抜プラグ	固着	ϕ	潤滑油の交換ができず，油の劣化，コンタミネーションなどが変化して故障，損傷を起こす原因となる.		
	破壊	ϕ			

付表 1　コンプレッサの FMEA (8/9)

部品名	故障モード	論理値	挙動		
			Pg コンプレッサ出力	P1 方向制御弁入力	P0 シリンダ出力
吐出弁	開放	1	影響なし.	影響なし.	影響なし.
	閉止	0	空気を吐出できないため Pg は出力せず.	圧縮空気が供給されないので P1 は出力しない.	圧縮空気が供給されないので P0 は出力しない.
	詰まり	0			
	外部リーク	0	吐出した空気が漏れ，Pg は出力せず.		
		1	吐出した空気が漏れるが Pg には影響がない.	影響なし.	影響なし.
	内部リーク	0		圧縮空気が供給されないので P1 は出力しない.	圧縮空気が供給されないので P0 は出力しない.
		1	吐出した空気が漏れるが Pg には影響がない.	影響なし.	影響なし.
潤滑関係	潤滑油温度上昇	0	軸受，摺動部の焼付き→機械損傷→異音, 騒音やがてはロータの回転位置が変化して接触事故の原因となる. 接触事故が発生したら圧縮空気は供給されなくなる.	圧縮空気が供給されないので P1 は出力しない.	圧縮空気が供給されないので P0 は出力しない.
	潤滑油圧力上昇	0	大事故につながる. ＊現在のところ起こる現象・原因不明.	圧縮空気が供給されないので P1 は出力しない.	圧縮空気が供給されないので P0 は出力しない.
	潤滑油供給できず	0	各部品や配管内に油が付着し時間が経過すると劣化しコンポーネントの故障の原因なり機能停止して圧縮空気が供給されない.	圧縮空気が供給されないので P1 は出力しない.	圧縮空気が供給されないので P0 は出力しない.

付表 1　コンプレッサの FMEA (9/9)

部品名	故障モード	論理値	挙動		
			Pg コンプレッサ出力	P1 方向制御弁入力	P0　シリンダ出力
冷却水関係	冷却水の温度上昇（急激な温度上昇）	0	ロータ接触事故が発生したら圧縮空気は供給されなくなるので Pg は感知しなくなってしまう.	圧縮空気が供給されないので P1 は出力しない.	圧縮空気が供給されないので P0 は出力しない.
冷却水関係	冷却水の温度低下（過冷却）	0	圧縮機内の異常摩耗が発生する. 性能低下のみであるが, Pg についてはすぐに影響はないが, 時間の経過により Pg は感知しなくなる.	—	—

付表 2　アフタークーラの FMEA(1/3)

部品名	故障モード	論理値	挙動		
			機器	P1 方向制御弁入力	P0 シリンダ出力
水室カバー	破壊	ϕ	冷却水が漏れ，冷却機能を果たさなくなるが，高温の圧縮空気が流れるため各機器の故障の原因となる可能性がある.	圧縮空気が供給されるので P1 は出力される. ＊一定時間経過すると機器の故障を招く可能性がある.	圧縮空気が供給されるので P1 は出力される.
	亀裂	1	亀裂の大きさが小さいのでアフタークーラの任務には影響がない．従って，Pg は出力される.	影響なし.	影響なし.
		1	亀裂の大きさが冷却水が漏れる程度であるため圧縮空気の冷却に影響がある.		
外筒	破壊	0	圧縮空気が大気に排出されてしまう．冷却する圧縮空気が大気に排出されてしまうので任務を果たせなくなる.	圧縮空気が供給されないので P1 は出力しない.	圧縮空気が供給されないので P0 は出力しない.
	変形	1	影響なし.	影響なし.	影響なし.
パッキン（冷却水出入口側）	破壊	0	冷却水が圧縮空気の通路に入ってしまい，流れなくなってしまう.	圧縮空気が供給されないので P1 は出力しない.	圧縮空気が供給されないので P0 は出力しない.
	亀裂	1	亀裂の大きさが小さいのでアフタークーラの任務には影響がない．従って，Pg は出力される.	影響なし.	影響なし.
		ϕ	亀裂の大きさが小さいく冷却水が漏れるがアフタークーラの任務には影響がない．従って，Pg は出力される.		
パッキン（ハウジング側）	破壊，亀裂	1	影響なし.		
ハウジング	破壊	0	圧縮空気が大気に排出されてしまい，次の機器へ供給できない.	圧縮空気が供給されないので P1 は出力しない.	圧縮空気が供給されないので P0 は出力しない.

付表 2　アフタークーラの FMEA(2/3)

部品名	故障モード	論理値	挙動		
			機器	P1 方向制御弁入力	P0 シリンダ出力
ハウジング	亀裂	1	亀裂の大きさが小さいのでアフタークーラの任務には影響がない．従って，Pg は出力される．	影響なし．	影響なし．
ハウジング	亀裂	ϕ	亀裂の大きさが小さいく圧縮空気が漏れるがアフタークーラの任務には影響がない．従って，Pg は出力される．	影響なし．	影響なし．
伝熱体アッセンブリ	破壊	0	冷却水が外筒内に漏れて充満してしまい，圧縮空気が流れなくなり，Pg は出力されない．	圧縮空気が供給されないので P1 は出力しない．	圧縮空気が供給されないので P0 は出力しない．
	亀裂	1	亀裂の大きさが小さいのでアフタークーラの任務には影響がない．従って，Pg は出力される．	影響なし．	影響なし．
		ϕ	亀裂の大きさが小さいく冷却水が漏れるが，圧縮空気の量，湿度に影響がでるが Pg は出力される．	湿度の高い圧縮空気が流れるので機器の故障を招く可能性がある．	影響なし．
ドレン弁	開かない（ハンドル）	1	圧縮空気が冷却され次の機器へ供給される．従って，Pg は出力される． ＊ドレンが溜まった時に排出できないので機器の故障原因となる	影響なし．	影響なし．
	閉じない（ハンドル）	0	ドレン排出口から圧縮空気が排出されてしまい，Pg は出力されない．	圧縮空気が供給されないので P1 は出力しない．	圧縮空気が供給されないので P0 は出力しない．
	固着（弁体）開側	0	ドレン排出口から圧縮空気が排出されてしまい，Pg は出力されない．		

付表 2　アフタークーラの FMEA(3/3)

部品名	故障モード	論理値	挙動		
			機器	P1 方向制御弁入力	P0 シリンダ出力
ドレン弁	固着（弁体）閉側	1	圧縮空気が冷却され次の機器へ供給される．従って，Pg は出力される． ＊ドレンが溜まった時に排出できないので機器の故障原因となる．	影響なし．	影響なし．
ドレン弁	破損	0	圧縮空気が冷却され次の機器へ供給される． 従って，Pg は出力される． ＊ドレンが溜まった時に排出できないので機器の故障原因となる．	影響なし．	影響なし．
ドレン弁	亀裂	1	亀裂の大きさが小さいのでアフタークーラの任務には影響がない． 従って，Pg は出力される． ＊ドレンが溜まった時に排出できないので機器の故障原因となる．	影響なし．	影響なし．
		ϕ	亀裂の大きさが小さいく，圧縮空気が漏れるが Pg は出力される．	圧縮空気の量が少ないが P1 は出力する．	P0 の動作が鈍くなる．

付表 3　ドレンセパレータの FMEA(1/2)

部品名	故障モード	論理値	挙動		
			機器	P1 方向制御弁入力	P0　シリンダ出力
ボディ	破壊	0	圧縮空気が大気中に排出され機器の任務を果たすことができない.	圧縮空気が供給されないので P1 は出力しない.	圧縮空気が供給されないので P0 は出力しない.
	亀裂	1	亀裂の大きさが小さいため亀裂部から空気が漏れるが影響はない.	影響なし.	影響なし.
		ϕ	亀裂の大きさが空気漏れを発生させる程度であるため, 圧縮空気排出量に影響がある.	圧縮空気の量が少ない.	P0 が要求性能通り出力しない.
O リング	破壊	ϕ	破壊箇所から圧縮空気が漏れるが効率の低下で機器の任務に影響は少ない.		
エレメント	目詰まり	1	目詰まりの量が少ないため, 機器の任務には影響がない.	影響なし.	影響なし.
		ϕ	目詰まりの量ある程度あるので, 圧縮空気の流量が少なくなり, 機器の機能が低下する.	圧縮空気の量が少ない.	P0 が要求性能通り出力しない.
		0	エレメント全てが目詰まりしたので圧縮空気が流れなくなるので, 機器の任務を果たすことができなくなる.	圧縮空気が供給されないので P1 は出力しない.	圧縮空気が供給されないので P0 は出力しない.
ケース	破壊	0	圧縮空気が大気中に排出され機器の任務を果たすことができない.	圧縮空気が供給されないので P1 は出力しない.	圧縮空気が供給されないので P0 は出力しない.
	亀裂	1	亀裂の大きさが小さいため亀裂部から空気が漏れるが影響はない.	影響なし.	影響なし.
		ϕ	亀裂の大きさが空気漏れを発生させる程度であるため, 圧縮空気排出量に影響がある.	圧縮空気の量が少ない.	P0 が要求性能通り出力しない.

付表 3　ドレンセパレータの FMEA(2/2)

部品名	故障モード	論理値	挙動		
			機器	P1 方向制御弁入力	P0　シリンダ出力
O リング	破壊	φ	破壊箇所から圧縮空気が漏れるが効率の低下で機器の任務に影響は少ない.	圧縮空気の量が少ない.	P0 が要求性能通り出力しない.
ドレン排出弁	開放	1	圧縮空気がドレン弁から排出されるので，機器の任務が喪失する.	圧縮空気が供給されないので P1 は出力しない.	圧縮空気が供給されないので P0 は出力しない.
	閉止	1	ドレンが溜まっても排出されないので，機器としての任務は喪失する.	影響なし.	影響なし.
	詰まり	1	ドレンが弁から排出されないので，機器の任務が喪失する. ＊ドレンが溜まるので機器の故障・トラブルの原因となる.		

付表 4　タンクの FMEA(1/2)

部品名	故障モード	論理値	挙動		
			機能	P1 方向制御弁入力	P0 シリンダ出力
タンク	破壊	0	圧縮空気が貯蔵されなくなり，供給されなくなる．機器としての任務を喪失する．	圧縮空気が供給されないので P1 は出力しない．	圧縮空気が供給されないので P0 は出力しない．
	亀裂	1	亀裂の大きさが小さいため亀裂部から空気が漏れるが影響はない．	影響なし．	影響なし．
		ϕ	亀裂の大きさが空気漏れを発生させる程度であるため，圧縮空気排出量に影響がある．	圧縮空気の量が少ない．	P0 が要求性能通り出力しない．
	変形	0	機器としての任務に影響はない	影響なし．	影響なし．
空気入口	破壊	0	圧縮空気が大気に排出され，貯蔵されなくなる．機器としての任務を喪失する．	圧縮空気が供給されないので P1 は出力しない．	圧縮空気が供給されないので P0 は出力しない．
	詰まり	0			
空気出口	破壊	0			
	詰まり	0	圧縮空気が大気に排出され，次の機器に供給されなくなる．		
マンホール	破壊	0	圧縮空気が大気に排出され，貯蔵されなくなる．機器としての任務を喪失する．		
	亀裂	1	亀裂の大きさが小さいため亀裂部から空気が漏れるが影響はない．	影響なし．	影響なし．
		ϕ	亀裂の大きさが空気漏れを発生させる程度であるため，圧縮空気排出量に影響がある．	圧縮空気の量が少ない．	P0 が要求性能通り出力しない．

付表 4　タンクの FMEA(2/2)

部品名	故障モード	論理値	挙動		
			機能	P1 方向制御弁入力	P0 シリンダ出力
圧力計	動作しない	1	現在の圧力値を示さないので機器としての任務は喪失する.	圧縮空気の供給には影響はない.	影響なし.
	破壊	1	現在の圧力値を示さないので機器としての任務は喪失する.	圧縮空気の供給には影響はない. ＊圧力が高くなり過ぎたなどを感知できなく安全を脅かす可能性あり.	影響なし.
安全弁	開放	0	圧縮空気が排出されるので，機器の任務が喪失する.	圧縮空気が供給されないのでP1は出力しない.	圧縮空気が供給されないので P0 は出力しない.
	閉止	1	弁が開かないので機器としての任務は喪失する. 圧縮空気の供給には影響はない.	影響なし.	影響なし.
	詰まり	1	弁の開閉が行われないので機能が喪失される．圧縮空気の供給には影響はない.	—	—
ドレン排出弁	開放	0	圧縮空気がドレン弁から排出されるので，機器の任務が喪失する.	圧縮空気が供給されないのでP1は出力しない.	圧縮空気が供給されないので P0 は出力しない.
	閉止	1	ドレンが溜まっても排出されないので，機器としての任務は喪失する.	影響なし.	影響なし.
	詰まり	1	ドレンが弁から排出されないので，機器の任務が喪失する.		

付表 5　ドライヤの FMEA（1/2）

部品名	故障モード	論理値	挙動		
			機能	P1 方向制御弁入力	P0 シリンダ出力
エアリヒータ	破損	0	本来の役割である圧縮空気の冷却がなされない.	圧縮空気が供給されないので P1 は出力しない.	圧縮空気が供給されないので P0 は出力しない.
	亀裂	1	亀裂の大きさが小さいため亀裂部から空気が漏れるが影響はない．しかし，1 次側の空気と 2 次側の空気が混ざり本来に役割である本来の空気の湿度が得られない.	影響なし.	影響なし.
		ϕ	亀裂の大きさが大きい場合に 1 次側の空気と 2 次側の空気が混ざり本来に役割である空気の乾燥がなされず，各種コンポーネントの故障につながる.	圧縮空気が供給されないので P1 は出力しない.	P0 が要求性能通り出力しない.
		0	1 次側の空気と 2 次側の空気が混ざり本来に役割である空気の乾燥がなされない.	圧縮空気が供給されないので P1 は出力しない.	P0 が要求性能通り出力しない.
	変形	1	機器としての任務に影響はない.	影響なし.	影響なし.
エアクーラ	破損	0	本来の役割である圧縮空気の冷却がなされない.	圧縮空気が供給されないので P1 は出力しない.	圧縮空気が供給されないので P0 は出力しない.
	冷却されない	ϕ	本来の役割である圧縮空気の冷却がなされない.	P1 への影響は直ぐにはないが機器の故障につながる.	P0 への影響は直ぐにはないが機器の故障につながる.
	動作しない	ϕ	本来の役割である圧縮空気の冷却がなされない.	P1 への影響は直ぐにはないが機器の故障につながる.	P0 への影響は直ぐにはないが機器の故障につながる.
オートドレン	破損	1	ドレンが排出できなくなる.	影響なし.	影響なし.
	オートドレンが機能しない	ϕ	ドレンが排出できなくなる.	P1 への影響は直ぐにはないが機器の故障につながる.	P0 への影響は直ぐにはないが機器の故障につながる.
	オートドレンが開放されたまま	ϕ	ドレンが排出されたままで，圧縮空気も放出されてしまう.	圧縮空気がドレンと一緒に排出されているので，圧縮空気供給されないので P1 は出力しない.	圧縮空気がドレンと一緒に排出されているので，圧縮空気供給されないので P1 は出力しない.

付表 5　ドライヤの FMEA（2/2）

部品名	故障モード	論理値	挙動		
			機能	P1 方向制御弁入力	P0 シリンダ出力
オートドレン	亀裂	1	亀裂が小さくドレン排出に影響がない.	影響なし.	影響なし.
		ϕ	ドレンが排出されたままで，圧縮空気も放出されてしまう.	圧縮空気がドレンと一緒に排出されているので，圧縮空気供給されないので P1 は出力しない.	圧縮空気がドレンと一緒に排出されているので，圧縮空気供給されないので P1 は出力しない.
	変形	1	変形部分が機能に関係がない.	影響なし.	影響なし.
蒸発器	破損	1	冷却が不能となり，ドレンとして水分を排出することができない.	圧縮空気は供給されるので P1 の出力には影響しない.	圧縮空気は供給されるので P0 の出力には影響しない.
	冷却されない	ϕ	冷却が不能となり，ドレンとして水分を排出することができない.	P1 への影響は直ぐにはないが機器の故障につながる.	P0 への影響は直ぐにはないが機器の故障につながる.

付表 6　フィルタの FMEA(1/4)

部品名	故障モード	論理値	挙動		
			機器	P1 方向制御弁入力	P0 シリンダ出力
プレートカバー	破損（破壊） 変形 亀裂 異物付着	1	影響なし.	影響なし.	影響なし.
ボディ	破損（破壊）	0	破壊により圧縮空気が大気に排出されてしまうのでフィルタとしての機能が果たせなくなる.	圧縮空気が供給されないので P1 は出力しない.	圧縮空気が供給されないので P0 は出力しない.
	変形	1	影響なし.	影響なし.	影響なし.
	亀裂	1	亀裂の大きさが小さいため亀裂部から空気が漏れるが影響はない.	影響なし.	影響なし.
		ϕ	亀裂の大きさが空気漏れを発生させる程度であるため，圧縮空気排出量に影響がある.	圧縮空気の量が少ない.	P0 が要求性能通り出力しない.
	異物付着	1	影響なし.	影響なし.	影響なし.
	詰まり	0	圧縮空気の出入口，通路に詰まりが発生した場合は，圧縮空気が流れないのでフィルタの機能を果たすことができなくなる.	圧縮空気が供給されないので P1 は出力しない.	圧縮空気が供給されないので P0 は出力しない.
O リング	破損（破壊） 亀裂	1	破損部から圧縮空気の漏れが発生するが，機能には影響は無い.	破損部から圧縮空気の漏れが発生するが, 圧縮空気が方向制御弁に供給されるので P1 の出力には影響はない.	圧縮空気漏れが発生しているので P0 が要求性能通り出力しない.
	変形 異物付着	1	影響なし.	影響なし.	影響なし.
ディフレクタ	固着	1	保全時に取り外しができなくなるが，機能上には影響は無い.	影響なし.	影響なし.

付表 6　フィルタの FMEA(2/4)

部品名	故障モード	論理値	挙動		
			機能	P1 方向制御弁入力	P0 シリンダ出力
ディフレクタ	破壊	1	圧縮空気が竜巻状にならないので圧縮空気の供給速度が低下する.		圧縮空気漏れが発生しているので，P0 が要求性能通り出力しない.
ディフレクタ	固着	1	保全時に取り外しができなくなるが，機能上には影響は無い.	影響なし.	影響なし.
	破壊	1	圧縮空気が竜巻状にならないので圧縮空気の供給速度が低下する.		圧縮空気漏れが発生しているので，P0 が要求性能通り出力しない.
ディフレクタ	亀裂 変形 異物付着	1	影響なし.	影響なし.	影響なし.
バッフル	破壊	ϕ	圧縮空気がフィルタを通さずに 2 次側（出口）へ流れてしまうので機能を果たせなくなる.	圧縮空気が供給され P1 は出力されるが，清浄度の悪い圧縮空気なので，レギュレータ，ルブリケータなどの故障の原因となる.	動作に影響がないが，P1 同様に，各種コンポーネントの故障の原因となる.
	亀裂	1	亀裂の大きさが小さいため亀裂部から圧縮空気が 2 次側（出口）へ流れてしまう場合や，ボウルに溜まる可能性があるが機能には影響はすくない.	影響なし ＊亀裂の場所によっては，清浄度の悪い圧縮空気なので，レギュレータ，ルブリケータなどの故障の原因となる.	影響なし ＊亀裂の場所によっては，P1 同様に，各種コンポーネントの故障の原因となる.
		ϕ	亀裂の大きさが大きいため亀裂部から圧縮空気が大量に 2 次側（出口）へ流れてしまう場合や，ボウルに溜まる可能性があるが機能低下する可能性がある.	圧縮空気が供給され P1 は出力されるが，清浄度の悪い圧縮空気なので，レギュレータ，ルブリケータなどの故障の原因となる.	動作に影響がないが，P1 同様に，各種コンポーネントの故障の原因となる.
ボウル	破壊	0	圧縮空気が大気に排出され，機能が喪失される.	圧縮空気が供給されないので P1 は出力しない.	圧縮空気が供給されないので P0 は出力しない.
	破損	0	破壊箇所が大きいので圧縮空気が大気に排出され，機能が喪失する.		

付表 6　フィルタの FMEA(3/4)

部品名	故障モード	論理値	挙動		
			機能	P1 方向制御弁入力	P0 シリンダ出力
ボウル	破損	ϕ	破壊箇所が小さいので圧縮空気が大気に排出少ないので，機能の喪失までは至らない.	破損部から圧縮空気の漏れが発生するが, 圧縮空気が方向制御弁に供給されるので P1 の出力には影響はない.	圧縮空気漏れが発生しているので P0 の動作少々鈍くなる.
	亀裂	1	亀裂の大きさが小さいため亀裂部から空気が漏れるが影響はない.	影響なし.	影響なし.
		ϕ	亀裂の大きさが空気漏れを発生させる程度であるため，圧縮空気排出量に影響がある.	圧縮空気の量が少ない.	P0 が要求性能通り出力しない.
	変形	1	影響なし.	影響なし.	影響なし.
ボウルガード	破壊 破損 亀裂 変形	1	ボウルをガードする機能は喪失する.	影響なし.	影響なし.
バッフル	変形	1	影響なし.		
	固着	1	保全時に取り外しができなくなるが，機能上には影響は無い.		
フィルタエレメント	破壊	1	空気清浄機能が喪失するので機能を喪失する.	P1 は出力するが，清浄度の悪い圧縮空気なので，レギュレータ，ルブリケータなどの故障の原因となる.	動作に影響がないが, P1 同様に, 各種コンポーネントの故障の原因となる.
	目詰まり	0	空気清浄機能が喪失するので機能を喪失する.	フィルタエレメントが 90%以上塵埃などで, 目詰まりしたら方向制御弁に圧縮空気が供給されないので P1 は出力しない.	圧縮空気が供給されないので P0 は出力しない.
		ϕ	空気清浄機能が低下する.	圧縮空気の流量・圧力が減少するが, 方向制御弁には圧縮空気が供給されるので P 1 は出力される.	圧縮空気の流量が少ないので, P0 の動作鈍くなる.

付表 6　フィルタの FMEA(4/4)

部品名	故障モード	論理値	挙動		
			機能	P1 方向制御弁入力	P0　シリンダ出力
ドレン排出弁	開放	0	圧縮空気がドレン弁から排出されるので，機器の任務が喪失する.	圧縮空気が供給されないので P1 は出力しない.	圧縮空気が供給されないので P0 は出力しない.
	閉止	1	ドレンが溜まっても排出されないので，機器としての任務は喪失する.	影響なし.	影響なし.
	詰まり	1	ドレンが弁から排出されないので，機器の任務が喪失する. ＊ドレンが溜まるので機器の故障・トラブルの原因となる.		

付表 7　レギュレータの FMEA(1/4)

部品名	故障モード	論理値	挙動		
			機　　器	P1 方向制御弁入力	P0 シリンダ出力
プレートカバー	破損（破壊）	1	影響なし.	影響なし.	影響なし.
	変形				
	亀裂				
	異物付着				
ボディ	破損（破壊）	0	破壊により圧縮空気が大気に排出されてしまうのでレギュレータとしての機能が果たせなくなる.	圧縮空気が供給されないのでP1は出力しない.	圧縮空気が供給されないので P0 は出力しない.
	変形	1	影響なし.	影響なし.	影響なし.
	亀裂	1	亀裂の大きさが小さいため亀裂部から空気が漏れるが影響はない.		
		ϕ	亀裂の大きさが空気漏れを発生させる程度であるため，圧縮空気排出量に影響がある.	圧縮空気の量が少ない.	P0 が要求性能通り出力しない.
	異物付着	1	影響なし.	影響なし.	影響なし.
	詰まり	0	圧縮空気の出入口，通路に詰まりが発生した場合は，圧縮空気が流れないのでレギュレータの機能を果たすことができなくなる.	圧縮空気が供給されないのでP1は出力しない.	圧縮空気が供給されないので P0 は出力しない.
バルブ	異物のかみ込み ゴムライニング面の損傷	ϕ	ハンドルを回して調節ばねをゆるめての２次側圧力が完全に下がらない.	圧縮空気は供給されるが設定圧力ではない.	P0 が要求性能通り出力しない.

付表 7　レギュレータの FMEA(2/4)

部品名	故障モード	論理値	挙動		
			機　　器	P1 方向制御弁入力	P0 シリンダ出力
バルブ	固着，破壊	1	圧力の調整ができない.	ハンドルの状況が設定圧力なら圧縮空気が供給され影響なし.	影響なし.
		ϕ		ハンドルの状況が設定圧力ではないが圧縮空気が供給され影響なし.	P0 が要求性能通り出力しない.
バルブスプリング	折損	ϕ	ハンドルを回して調節ばねをゆるめての２次側圧力が完全に下がらない.	圧縮空気は供給されるが設定圧力ではない.	P0 が要求性能通り出力しない.
	破壊	1	圧力の調整ができない.	ハンドルの状況が設定圧力なら圧縮空気が供給され影響なし.	影響なし.
		ϕ		ハンドルの状況が設定圧力ではないが圧縮空気が供給され影響なし.	P0 が要求性能通り出力しない.
		0		ハンドルの状況が設定圧力値 0MPa であるので圧縮空気は供給されない.	圧縮空気が供給されないので P0 は出力しない.
ダイヤフラム	破損（破れ）	1	圧力の調整ができない.	ハンドルの状況が設定圧力なら圧縮空気が供給され影響なし.	影響なし.
		ϕ		ハンドルの状況が設定圧力ではないが圧縮空気が供給され影響なし.	P0 が要求性能通り出力しない.
		0		ハンドルの状況が設定圧力値 0MPa であるので圧縮空気は供給されない.	圧縮空気が供給されないので P0 は出力しない.
		ϕ	圧縮空気が漏れる.	破損の程度によって圧縮空気の漏れ量が変化するが，圧縮空気は供給される.	P0 が要求性能通り出力しない.
調圧スプリング	破損（折損）	1	圧力の調整ができない.	ハンドルの状況が設定圧力なら圧縮空気が供給され影響なし.	影響なし.
		ϕ		ハンドルの状況が設定圧力ではないが圧縮空気が供給され影響なし.	P0 が要求性能通り出力しない.
		0		ハンドルの状況が設定圧力値 0MPa であるので圧縮空気は供給されない.	圧縮空気が供給されないので P0 は出力しない.

付表 7　レギュレータの FMEA(3/4)

部品名	故障モード	論理値	挙動		
			機　　器	P1 方向制御弁入力	P0　シリンダ出力
アジャスティングスクリュウ	固着	1	ノブが回転しなくなり，圧力の調節ができなくなる.	ハンドルの状況が設定圧力なら圧縮空気が供給され影響なし.	影響なし.
		ϕ		ハンドルの状況が設定圧力ではないが圧縮空気が供給され影響なし.	P0 が要求性能通り出力しない.
		0		ハンドルの状況が設定圧力値 0MPa であるので圧縮空気は供給されない.	圧縮空気が供給されないので P0 は出力しない.
リングナット	破損（破壊）	1	影響なし.	影響なし.	影響なし.
	変形				
	亀裂				
	異物付着				
カバー	破損（破壊）	1	影響なし.	影響なし.	影響なし.
	変形				
	亀裂				
	異物付着				
ノブ	破損,固着	1	ノブが回転しなくなり，圧力の調節ができなくなる.	ハンドルの状況が設定圧力なら圧縮空気が供給され影響なし.	影響なし.
		ϕ		ハンドルの状況が設定圧力ではないが圧縮空気が供給され影響なし.	P0 が要求性能通り出力しない.
		0		ハンドルの状況が設定圧力値 0MPa であるので圧縮空気は供給されない.	圧縮空気が供給されないので P0 は出力しない.

付表 7　レギュレータの FMEA(4/4)

部品名	故障モード	論理値	挙動		
			機　　器	P1 方向制御弁入力	P0　シリンダ出力
圧力計	動作しない 高い値にずれる 低い値にずれる	φ	圧力調整した値が分からなくなる.	ハンドルの状況が設定圧力ではないが圧縮空気が供給され影響なし.	P0 が要求性能通り出力しない.

付表 8　ルブリケータの FMEA(1/2)

部品名	故障モード	論理値	挙動		
			機　　器	P1 方向制御弁入力	P0 シリンダ出力
プレートカバー	破損（破壊）	1	影響なし.	影響なし.	影響なし.
	変形				
	亀裂				
	異物付着				
ボディ	破損（破壊）	0	破壊により圧縮空気が大気に排出されてしまうのでルブリケータとしての機能が果たせなくなる.	圧縮空気が供給されないので P1 は出力しない.	圧縮空気が供給されないので P0 は出力しない.
	変形	1	影響なし.	影響なし.	影響なし.
	亀裂	1	亀裂の大きさが小さいため亀裂部から空気が漏れるが影響はない.		
		ϕ	亀裂の大きさが空気漏れを発生させる程度であるため，圧縮空気排出量に影響がある.	圧縮空気の量が少ないが P1 は出力する.	P0 が要求性能通り出力しない.
	異物付着	1	影響なし.	影響なし.	影響なし.
	詰まり	0	圧縮空気の出入口，通路に詰まりが発生した場合は，圧縮空気が流れないのでルブリケータの機能を果たすことができなくなる.	圧縮空気が供給されないので P1 は出力しない.	圧縮空気が供給されないので P0 は出力しない.
可変絞り	破損	1	潤滑油の濃度を調整できなくなる.	影響なし.	影響なし.
ボウル	破壊	0	圧縮空気が大気に排出され，機能が喪失される.	圧縮空気が供給されないので P1 は出力しない.	圧縮空気が供給されないので P0 は出力しない.
	破損	1	破壊箇所の大きいので潤滑油が漏れ機能が喪失する.	潤滑油が供給されないのみなので，P1 には影響がない. ＊潤滑効果がなくなるので故障の原因となる可能性あり.	潤滑油が供給されないのみで P0 は出力しない. ＊潤滑効果がなくなるので故障の原因となる可能性あり.

付表 8　ルブリケータの FMEA(2/2)

部品名	故障モード	論理値	挙動		
			機　　器	P1 方向制御弁入力	P0 シリンダ出力
ボウル	破壊	0	圧縮空気が大気に排出され，機能が喪失される.	圧縮空気が供給されないので P1 は出力しない.	圧縮空気が供給されないので P0 は出力しない.
	破損	1	破壊箇所が小さいので 潤滑油が漏れ機能の低下となる.	破損部から潤滑油漏れが発生するが, 潤滑油は方向制御弁に供給されるので P1 の出力には影響はない.	影響なし.
	亀裂	1	亀裂の大きさが小さいため亀裂部から潤滑油が漏れるが影響はない.	影響なし.	影響なし.
	変形	1	影響なし.		
ボウルガード	破壊 破損 亀裂 変形	1	ボウルをガードする機能は喪失する.		
導油管	詰まり，破壊	1	潤滑油を供給できないので機能を喪失する.	P1 の出力には影響がない. ＊潤滑油が供給されないので方向制御弁の故障の原因となる.	P0 の出力には影響がない. ＊潤滑油が供給されないので方向制御弁の故障の原因となる.
	潤滑油不足，なし				
アジャステイングドーム	破壊，詰まり	1			
	詰まり				
フローガイド	破損	ϕ	破壊箇所から圧縮空気･潤滑油が漏れる. 機能を喪失する.	圧縮空気の量が少ないが P1 は出力する.	P0 が要求性能通り出力しない.
フィルプラグ	破壊，固着	1	潤滑油を供給できないので機能を喪失する.	影響なし.	影響なし.

付表 9　方向制御弁（シングルソレノイドバルブ）の FMEA(1/3)

部品名	故障モード	論理値	挙動	
			機　　器	P0 シリンダ出力
本体	破壊	0	圧縮空気が大気に排出されてしまうので，空気の方向制御ができなるくなる.	圧縮空気が供給されないので，P0 は出力されない.
	詰まり（空気通路） 出口ポート 入力ポート 排気ポート	0	圧縮空気を供給できなくなる.	
	破損	0	空気通路部分が破損した場合は，圧縮空気を供給できなくなるので機能を喪失する.	
		1	破損部分が小さい又は空気通路に関係の無い部分のため影響はない.	影響なし.
		ϕ	破損部分が小さく，空気通路部分なので圧縮空気が漏れる.	圧縮空気の供給量に変化があるので P0 の出力が正常ではない.
	亀裂	1	亀裂の大きさが小さいため亀裂部から空気が漏れるが影響はない.	影響なし.
		ϕ	亀裂の大きさが空気漏れを発生させる程度であるため，圧縮空気排出量に影響がある.	圧縮空気の供給量に変化があるので P0 が要求性能通り出力しない.
	変形	1	影響なし.	影響なし.
キャップ	破壊	0	スプール動作時に，ピストン B がはずれ，圧縮空気が漏れるのと，圧縮空気の流れを切換えることができない.	圧縮空気が供給されないので，P0 は出力されない.
		ϕ	破壊の仕方によっては，片側にスプールが動作してしまい，そのご切換ができない.	圧縮空気の供給量に変化があるので P0 が要求性能通り出力しない.
スプール	破壊	0	圧縮空気の流れの方向を切換ることができなくなるので機能を喪失する.	圧縮空気が供給されないので，P0 は出力されない.
	固着	0		
	切換わらない	0		
ピストン A ピストン B	固着，破壊 動作しない	0	固着によりスプールを押す動作ができなくなるので，圧縮空気の流れの方向を切り換えることができなくなり，機能を喪失する.	圧縮空気が供給されないので，P0 は出力されない.

付表 9　シングルソレノイドバルブの FMEA(2/3)

部品名	故障モード	論理値	挙動	
			機　　器	P0　シリンダ出力
シリンダ A シリンダ B	変形	0	シリンダ変形により，ピストン A，B を固着させてしまい，圧縮空気の流れの方向を切り換えることができなくなり，機能を喪失する．	圧縮空気が供給されないので，P0 は出力されない．
シール	変形	0	シールの変形により，スプールを固着させてしまい，圧縮空気の流れの方向を切り換えることができなくなり，機能を喪失する．	
O リング	破損	1	破損箇所からエアー漏れが発生するが，機能には影響がないが，効率に問題が発生する．	影響なし．
プランジャ	破壊 固着 動作しない	0	パイロットエアーが供給されず，スプールが動作しなくなる．従って，圧縮空気の流れの方向を切り換えることができなくなり，機能を喪失する．	圧縮空気が供給されないので，P0 は出力されない．
	異物混入	0	コイルが焼損しパイロットエアーが供給されず，スプールが動作しなくなる．従って，圧縮空気の流れの方向を切り換えることができなくなり，機能を喪失する．	
		ϕ	うなりが発生して動作に影響がでる．	圧縮空気の供給量に変化があるので P0 が要求性能通り出力しない．
プランジャばね	破損 折損	0	プランジャが動作してスプールが動作しても，定位置に復帰しない，従って，圧縮空気の流れの方向を切り換えることができなくなり，機能を喪失する．	圧縮空気が供給されないので，P0 は出力されない．
コイル	焼損	0	コイルが焼損しパイロットエアーが供給されず，スプールが動作しなくなる．従って，圧縮空気の流れの方向を切り換えることができなくなり，機能を喪失する．	圧縮空気が供給されないので，P0 は出力されない．
	短絡	ϕ	うなりが発生してプランジャの吸引力が低下して動作に影響がでる．	圧縮空気の供給量に変化があるので P0 が要求性能通り出力しない．

付表 9　シングルソレノイドバルブの FMEA(3/3)

部品名	故障モード	論理値	挙動	
			機　　器	P0 シリンダ出力
ケーブル	断線 誤配線	0	通電されず，プランジャが動作せず，圧縮空気の流れの方向を切り換えることができなくなり，機能を喪失する.	圧縮空気が供給されないので，P0 は出力されない.
パイロット圧通路	詰まり	0	パイロットエアーが供給されないので，スプールの切換ができなるので，機能を喪失する.	

付表 10　方向制御弁（ダブルソレノイドバルブ）の FMEA(1/3)

部品名	故障モード	論理値	挙動	
			コンポーネント	P0 シリンダ出力
本体	破壊	0	圧縮空気が大気に排出されてしまうので，空気の方向制御ができなるくなる．	圧縮空気が供給されないので，P0 は出力されない．
	詰まり（空気通路） 出口ポート 入力ポート 排気ポート	0	圧縮空気を供給できなくなる．	
	破損	0	空気通路部分が破損した場合は，圧縮空気を供給できなくなるので機能を喪失する．	
		1	破損部分が小さい又は空気通路に関係の無い部分のため影響はない．	影響なし．
		ϕ	破損部分が小さく，空気通路部分なので圧縮空気が漏れる．	圧縮空気の供給量に変化があるので P0 が要求性能通り出力されない．
	亀裂	1	亀裂の大きさが小さいため亀裂部から空気が漏れるが影響はない．	影響なし．
		ϕ	亀裂の大きさが空気漏れを発生させる程度であるため，圧縮空気排出量に影響がある．	圧縮空気の供給量に変化があるので P0 が要求性能通り出力されない．
	変形	1	影響なし．	影響なし．
スプール	破壊	0	圧縮空気の流れの方向を切換ることができなくなるので機能を喪失する．	圧縮空気が供給されないので，P0 は出力されない．
	固着	0		
	切換わらない	0		
ピストン A ピストン B	固着，破壊 動作しない	0	固着によりスプールを押す動作ができなくなるので，圧縮空気の流れの方向を切り換えることができなくなり，機能を喪失する．	圧縮空気が供給されないので，P0 は出力されない．
シリンダ A シリンダ B	変形	0	シリンダ変形により，ピストン A，B を固着させてしまい，圧縮空気の流れの方向を切り換えることができなくなり，機能を喪失する．	圧縮空気が供給されないので，P0 は出力されない．

付表 10　ダブルソレノイドバルブの FMEA(2/3)

部品名	故障モード	論理値	挙動	
			コンポーネント	P0　シリンダ出力
シール	変形	0	シールの変形により，スプールを固着させてしまい，圧縮空気の流れの方向を切り換えることができなくなり，機能を喪失する．	圧縮空気が供給されないので，P0 は出力されない．
O リング	破損	1	破損箇所からエアー漏れが発生するが，機能には影響がないが，効率に問題が発生する．	影響なし．
プランジャ A プランジャ B	破壊 固着 動作しない	0	パイロットエアーが供給されず，スプールが動作しなくなる．従って，圧縮空気の流れの方向を切り換えることができなくなり，機能を喪失する．	圧縮空気が供給されないので，P0 は出力されない．
プランジャ A プランジャ B	異物混入	0	コイルが焼損しパイロットエアーが供給されず，スプールが動作しなくなる．従って，圧縮空気の流れの方向を切り換えることができなくなり，機能を喪失する．	圧縮空気が供給されないので，P0 は出力されない．
		ϕ	うなりが発生して動作に影響がでる．	圧縮空気の供給量に変化があるので P0 が要求性能通り出力されない．
プランジャばね A プランジャばね B	破損 折損	0	プランジャが動作してスプールが動作しても，定位置に復帰しない，従って，圧縮空気の流れの方向を切り換えることができなくなり，機能を喪失する．	圧縮空気が供給されないので，P0 は出力されない．
コイル A コイル B	焼損	0	コイルが焼損しパイロットエアーが供給されず，スプールが動作しなくなる．従って，圧縮空気の流れの方向を切り換えることができなくなり，機能を喪失する．	圧縮空気が供給されないので，P0 は出力されない．
	短絡	ϕ	うなりが発生してプランジャの吸引力が低下して動作に影響がでる．	圧縮空気の供給量に変化があるので P0 の出力が正常ではない．
パイロット圧通路	詰まり	0	パイロットエアーが供給されないので，スプールの切換ができなるので，機能を喪失する．	圧縮空気が供給されないので，P0 は出力されない．

付表 10　ダブルソレノイドバルブの FMEA(3/3)

部品名	故障モード	論理値	挙動	
			機　　器	P0 シリンダ出力
ケーブル A ケーブル B	断線 誤配線	0	通電されず，プランジャが動作せず，圧縮空気の流れの方向を切り換えることができなくなり，機能を喪失する.	圧縮空気が供給されないので，P0 は出力されない.

付表 11　方向制御弁（ダブルソレノイドバルブ 3 ポジション（両側スプリング付））の FMEA(1/3)

部品名	故障モード	論理値	挙動	
			機　　器	P0 シリンダ出力
本体	破壊	0	圧縮空気が大気に排出されてしまうので，空気の方向制御ができなるくなる.	圧縮空気が供給されないので，P0 は出力されない.
	詰まり （空気通路） 出口ポート 入力ポート 排気ポート	0	圧縮空気を供給できなくなる.	
	破損	0	空気通路部分が破損した場合は，圧縮空気を供給できなくなるので機能を喪失する.	
		1	破損部分が小さい又は空気通路に関係の無い部分のため影響はない.	影響なし.
		ϕ	破損部分が小さく，空気通路部分なので圧縮空気が漏れる.	圧縮空気の供給量に変化があるので P0 が要求性能通り出力されない.
	亀裂	1	亀裂の大きさが小さいため亀裂部から空気が漏れるが影響はない.	影響なし.
		ϕ	亀裂の大きさが空気漏れを発生させる程度であるため，圧縮空気排出量に影響がある.	圧縮空気の供給量に変化があるので P0 が要求性能通り出力されない.
	変形	1	影響なし.	影響なし.
スプール	破壊	0	圧縮空気の流れの方向を切換ることができなくなるので機能を喪失する.	圧縮空気が供給されないので，P0 は出力されない.
	固着	0		
	切換わらない	0		

付表 11　ダブルソレノイドバルブ 3 ポジション（両側スプリング付）の FMEA(2/3)

部品名	故障モード	論理値	挙動	
			機　　器	P0 シリンダ出力
スプールスプリング A スプールスプリング B	破損 折損	0	プランジャが動作してスプールが動作しても，定位置に復帰しない，従って，圧縮空気の流れの方向を切り換えることができなくなり，機能を喪失する.	圧縮空気が供給されないので，P0 は出力されない.
ピストン A ピストン B	固着，破壊 動作しない	0	固着によりスプールを押す動作ができなくなるので，圧縮空気の流れの方向を切り換えることができなくなり，機能を喪失する.	圧縮空気が供給されないので，P0 は出力されない.
シリンダ A シリンダ B	変形	0	シリンダ変形により，ピストン A, B を固着させてしまい，圧縮空気の流れの方向を切り換えることができなくなり，機能を喪失する.	圧縮空気が供給されないので，P0 は出力されない.
シール	変形	0	シールの変形により，スプールを固着させてしまい，圧縮空気の流れの方向を切り換えることができなくなり，機能を喪失する.	圧縮空気が供給されないので，P0 は出力されない.
O リング	破損	1	破損箇所からエアー漏れが発生するが，機能には影響がないが，効率に問題が発生する.	影響なし.
プランジャ A プランジャ B	破壊 固着 動作しない	0	パイロットエアーが供給されず，スプールが動作しなくなる．従って，圧縮空気の流れの方向を切り換えることができなくなり，機能を喪失する.	圧縮空気が供給されないので，P0 は出力されない.
	異物混入	0	コイルが焼損しパイロットエアーが供給されず，スプールが動作しなくなる．従って，圧縮空気の流れの方向を切り換えることができなくなり，機能を喪失する.	
		ϕ	うなりが発生して動作に影響がでる.	圧縮空気の供給量に変化があるので P0 が要求性能通り出力されない.
コイル A コイル B	焼損	0	コイルが焼損しパイロットエアーが供給されず，スプールが動作しなくなる．従って，圧縮空気の流れの方向を切り換えることができなくなり，機能を喪失する.	圧縮空気が供給されないので，P0 は出力されない.
	短絡	ϕ	うなりが発生してプランジャの吸引力が低下して動作に影響がでる.	圧縮空気の供給量に変化があるので P0 の出力が正常ではない.

付表 11　ダブルソレノイドバルブ 3 ポジション（両側スプリング付）の FMEA(3/3)

部品名	故障モード	論理値	挙動	
			機　　器	P0　シリンダ出力
ボディブロック A ボディブロック B	破損	0	破損部分の大きいので，エアーが排出されてしまうので，圧縮空気の流れの方向を切り換えることができなくなり，機能を喪失する.	圧縮空気が供給されないので，P0 は出力されない.
		ϕ	破損部分が少々あるので，エアー漏れが起こる. 機能については性能が低下する.	圧縮空気の供給量に変化があるので P0 が要求性能通り出力されない.
		1	破損部分が小さいので，エアー漏れが起こる. 機能については性能が低下する.	微量であるため P0 の出力には影響がない.
パイロット圧通路	詰まり	0	パイロットエアーが供給されないので，スプールの切換ができなるので，機能を喪失する.	圧縮空気が供給されないので，P0 は出力されない
プランジャばね A プランジャばね B	破損 折損	0	プランジャが動作してスプールが動作しても，定位置に復帰しない，従って，圧縮空気の流れの方向を切り換えることができなくなり，機能を喪失する.	圧縮空気が供給されないので，P0 は出力されない.
ケーブル A ケーブル B	断線 誤配線	0	通電されず，プランジャが動作せず，圧縮空気の流れの方向を切り換えることができなくなり，機能を喪失する.	圧縮空気が供給されないので，P0 は出力されない.
ケーブル A ケーブル B	断線 誤配線	0	通電されず，プランジャが動作せず，圧縮空気の流れの方向を切り換えることができなくなり，機能を喪失する.	圧縮空気が供給されないので，P0 は出力されない.
ボディブロック A ボディブロック B	亀裂	1	亀裂の大きさが微量なので機能には影響がない.	影響なし.
		ϕ	亀裂の大きさが大きいので，エアー漏れが起こる. 機能については性能が低下する.	圧縮空気の供給量に変化があるので P0 が要求性能通り出力されない.

付表 12　スピードコントローラの FMEA(1/2)

部品名	故障モード	論理値	挙動	
			機　　器	P0 シリンダ出力
ボディ	破損（破壊）	0	破壊により圧縮空気が大気に排出されてしまうのでスピコンとしての機能が果たせなくなる.	圧縮空気が供給されないので P0 は出力しない.
	変形	1	影響なし.	影響なし.
	亀裂	1	亀裂の大きさが小さいため亀裂部から圧縮空気が漏れるが影響はない.	
		ϕ	亀裂の大きさが圧縮空気漏れを発生させる程度であるため，圧縮空気排出量に影響がある.	P0 の動作が要求性能通り出力しない.
	異物付着	1	影響なし.	影響なし.
	詰まり（出口，入口）	0	圧縮空気の出入口，通路に詰まりが発生した場合は，圧縮空気が流れないのでスピコンの機能を果たすことができなくなる.	圧縮空気が供給されないので P0 は出力しない.
ガスケット	破損，割れ	1	圧縮空気漏れを起こすが，スピコンの機能を低下させる.	P0 の動作が要求性能通り出力しない.
ロックナット	破損	1	速度設定を行い，速度を維持する役割である．ロックしなくても速度を維持することができる.	影響なし.
	固着	1	適切な速度設定で固着した場合は，機能を果たすので問題はない.	
		ϕ	要求速度設定以外の設定で固着している．機能には問題なし.	P0 の動作が要求性能通り出力しない.
		0	弁が閉じた状態で固着しているので，機能を果たすことができない.	圧縮空気が供給されないので P0 は出力しない.
弁シート	破損	ϕ	速度制御機能が喪失されるので， 機能を喪失する.	P0 の動作が要求性能通り出力しない.
	固着	1	適切な速度設定で固着した場合は，機能を果たすので問題はない.	影響なし.
		ϕ	要求速度設定以外の設定で固着している．機能には問題なし.	P0 の動作が要求性能通り出力しない.
		0	弁が閉じた状態で固着しているので，機能を果たすことができない.	圧縮空気が供給されないので P0 は出力しない.
弁シートばね	破損，折損	ϕ	自由流れの際の流量に影響があるが，機能についても問題なし.	P0 の動作が要求性能通り出力しない.

付表 12　スピードコントローラの FMEA(2/2)

部品名	故障モード	論理値	挙動	
			機　　器	P0 シリンダ出力
E 形止め輪	破損	1	影響なし.	影響なし.
	紛失			
ニードルガイド	固着	1	適切な速度設定で固着した場合は，機能を果たすので問題はない.	影響なし.
		ϕ	要求速度設定以外の設定で固着している．機能には問題なし.	P0 の動作が要求性能通り出力しない.
		0	弁が閉じた状態で固着しているので，機能を果たすことができない.	圧縮空気が供給されないので P0 は出力しない.
O リング	破損	ϕ	圧縮空気が漏れるが，機能は果たせる.	P0 の動作が要求性能通り出力しない.
つまみ	固着	1	適切な速度設定で固着した場合は，機能を果たすので問題はない.	影響なし.
		ϕ	要求速度設定以外の設定で固着している．機能には問題なし.	P0 の動作が要求性能通り出力しない.
		0	弁が閉じた状態で固着しているので，機能を果たすことができない.	圧縮空気が供給されないので P0 は出力しない.
	外れ	1	適切な速度設定で外れた場合は，機能を果たすので問題はない.	影響なし.
		ϕ	要求速度設定以外の設定で外れている．機能には問題なし.	P0 の動作が要求性能通り出力しない.
		0	弁が閉じた状態で外れているので，機能を果たすことができない.	圧縮空気が供給されないので P0 は出力しない.

付表 13　エアシリンダの FMEA（1/5）

部品名	故障モード	論理値	挙動	
			機　　器	P0 シリンダ出力
ロッドカバー	破壊	0	ピストンロッドが出力できなくなり，圧縮空気も大気に排出されてしまうので機能を喪失する．	圧縮空気が供給されないので P0 は出力しない．
	破損	1	破損箇所が小さく，圧縮空気の漏れも微量であるので機能は喪失しない．	影響なし．
		ϕ	破損箇所から，圧縮空気が漏れておりシリンダの動作に影響がある場所の破損であるので，機能低下する．	P0 の要求動作を満たさないが，動作はする．
		0	破損箇所が大きい又は機能喪失する部分の破損であるため，機能喪失する．破損箇所が大きい場合は圧縮空気が大気に排出される．	圧縮空気が供給されないので P0 は出力しない．
	亀裂	1	亀裂の大きさが小さいため亀裂部から空気が漏れるが影響はない．	影響なし．
		ϕ	亀裂の大きさが空気漏れを発生させる程度であるため，圧縮空気排出量に影響がある．	P0 の要求動作を満たさないが，動作はする．
	固着	1	シリンダチューブに固着して取り外しができなくなっても，機能には影響がない．	影響なし．
	詰まり	0	圧縮空気入力・出力ポートが詰まり圧縮空気が供給・排出できない．	圧縮空気供給されないので P0 は出力しない．
ブッシュ	変形	ϕ	変形量が大きい場合，タイロッドの動作を妨げる．	P0 の要求動作を満たさないが，動作はする．
	亀裂	1	亀裂の大きさが小さい場合は機能に影響は無い．	影響なし．
		ϕ	亀裂の大きさが空気漏れを発生させる程度である．	P0 の要求動作を満たさないが，動作はする．
	破損	ϕ	空気漏れを発生させる程度であるため，機能への影響は少ない．	P0 の要求動作を満たさないが，動作はする．
	固着	0	ピストンロッドへ固着した場合，ロッドが動作しなくなるので機能を喪失する．	ロッドが動作不能なので P0 は出力しない．
	偏芯	0	ピストンロッドと偏芯が発生した場合，偏芯量が大きいとロッドが動作しなくなるので，機能を喪失する．	ロッドが動作不能なので P0 は出力しない．

付表 13　エアシリンダの FMEA（2/5）

部品名	故障モード	論理値	挙動	
			機　　器	P0 シリンダ出力
ブッシュ	偏芯	ϕ	ピストンロッドと偏芯が発生した場合，偏芯量小さくロッドが動作するが，ロッド，ブッシュともに摩耗が発生する． その他機器の故障の原因となる．	P0 の要求動作を満たさないが，動作はする．
ロッドパッキン	破損（割れ）	0	破損箇所から圧縮空気が排出されパッキンの交換が必要となる．	圧縮空気が供給されないので P0 は出力しない．
		ϕ	破損箇所が小さいのでシリンダは動作するが性能低下する．	P0 の要求動作を満たさないが，動作はする．
ダストワイパ	破損（割れ）	0	破損箇所から圧縮空気が排出されダストワイパの交換が必要となる．	圧縮空気が供給されないので P0 は出力しない．
		ϕ	破損箇所が小さいのでシリンダは動作するが性能低下する．	P0 の要求動作を満たさないが，動作はする．
チューブ	破壊	0	圧縮空気も大気に排出されてしまうので機能を喪失する．	圧縮空気が供給されないので P0 は出力しない．
	破損	ϕ	破損箇所から，圧縮空気が漏れておりシリンダの動作に影響がある場所の破損であるので，機能低下する．	P0 の要求動作を満たさないが，動作はする．
		0	破損箇所が大きい又は機能喪失する部分の破損であるため，機能喪失する．破損箇所が大きい場合は圧縮空気が大気に排出される．	圧縮空気が供給されないので P0 は出力しない．
	亀裂	1	亀裂の大きさが小さいため亀裂部から空気が漏れるが影響はない．	影響なし．
		ϕ	亀裂の大きさが空気漏れを発生させる程度であるため，圧縮空気排出量に影響がある．	P0 の要求動作を満たさないが，動作はする．
	変形	0	変形箇所でピストンが停止してしまうので機能を喪失する．	ピストンが動作できないので，P0 は出力しない．
ロッドナット	破壊 破損 亀裂	1	影響なし．	影響なし．

付表 13　エアシリンダの FMEA（3/5）

部品名	故障モード	論理値	挙動	
			機　　器	P0 シリンダ出力
ロッドナット	変形	1	影響なし.	影響なし.
ピストンロッド	破壊	0	負荷を運ぶ機能であるので破壊の場合は機能を喪失する.	負荷を運ぶ機能が破壊されるので P0 は出力しない.
	破損	0		
	亀裂	1	亀裂の大きさが小さいので機能に影響は無い.	影響なし.
		ϕ	亀裂の大きさが大きいので負荷によっては破損する可能性がある.	P0 の要求動作を満たさないが，動作はする.
	変形	0	変形量が大きいのでロッドカバー等と接触して動作しなくなるので機能を喪失する.	ピストンが動作できないので，P0 は出力しない.
		ϕ	変形量が小さいのでロッドカバー等と接触して動作がぎごちなくなるので，機能が低下する.	P0 の要求動作を満たさないが，動作はする. ＊やがては故障を招く
	偏芯	0	ロッドカバーと偏芯が発生した場合，偏芯量が大きいとロッドが動作しなくなるので，機能を喪失する.	ロッドが動作不能なので P0 は出力しない.
		ϕ	ロッドカバーと偏芯が発生した場合，偏芯量小さくロッドが動作するが，ロッド，ロッドカバーともに摩耗が発生する. その他機器の故障の原因となる.	P0 の要求動作を満たさないが，動作はする.
ピストン R	破壊	0	負荷を運ぶ機能であるので破壊の場合は機能を喪失する.	負荷を運ぶ機能が破壊されるので P0 は出力しない.
	破損			
	亀裂	1	亀裂の大きさが小さいので機能に影響は無い.	影響なし.
		ϕ	亀裂の大きさが大きいので負荷によっては破損する可能性がある.	P0 の要求動作を満たさないが，動作はする.
	変形	0	変形量が大きいのでチューブ等と接触して動作しなくなるので機能を喪失する.	ピストンが動作できないので，P0 は出力しない.
		ϕ	変形量が小さいのでチューブ等と接触して動作がぎごちなくなるので，機能が低下する.	P0 の要求動作を満たさないが，動作はする. ＊やがては故障を招く
	偏芯	0	チューブと偏芯が発生した場合，偏芯量が大きいとピストンが動作しなくなるので，機能を喪失する.	ロッドが動作不能なので P0 は出力しない.
		ϕ	チューブと偏芯が発生した場合，偏芯量小さくピストンが動作するが，チューブとともに摩耗が発生する．その他機器の故障の原因となる.	P0 の要求動作を満たさないが，動作はする.

付表 13　エアシリンダの FMEA（4/5）

部品名	故障モード	論理値	挙動	
			機　　器	P0　シリンダ出力
ピストン R	固着	0	ピストンがチューブと固着して機能を喪失する.	ピストンが動作できないので，P0 は出力しない.
ピストン H	破壊 破損	0	負荷を運ぶ機能であるので破壊の場合は機能を喪失する.	負荷を運ぶ機能が破壊されるので P0 は出力しない.
	亀裂	1	亀裂の大きさが小さいので機能に影響は無い.	影響なし.
		ϕ	亀裂の大きさが大きいので負荷によっては破損する可能性がある.	P0 の要求動作を満たさないが，動作はする.
	変形	0	変形量が大きいのでチューブ, ヘッドカバーと接触して動作しなくなるので機能を喪失する.	ピストンが動作できないので，P0 は出力しない.
		ϕ	変形量が小さいのでチューブ･ヘッドカバーと接触して動作がぎごちなくなるので，機能が低下する.	P0 の要求動作を満たさないが，動作はする. ＊やがては故障を招く
	偏芯	0	チューブと偏芯が発生した場合, 偏芯量が大きいとピストンが動作しなくなるので，機能を喪失する.	ロッドが動作不能なので P0 は出力しない.
		ϕ	チューブと偏芯が発生した場合, 偏芯量小さくピストンが動作するが，チューブとともに摩耗が発生する. その他機器の故障の原因となる.	P0 の要求動作を満たさないが，動作はする.
	固着	0	ピストンがチューブと固着して機能を喪失する.	負荷を運ぶ機能が破壊されるので P0 は出力しない.
ピストンガスケット	破損	ϕ	エアー漏れが生じる，機能が低下する.	P0 の要求動作を満たさないが，動作はする.
ヘッドカバー	破壊	0	ピストンロッドが出力できなくなり, 圧縮空気も大気に排出されてしまうので機能を喪失する.	圧縮空気が供給されないので P0 は出力しない.
	破損	1	破損箇所が小さく, 圧縮空気の漏れも微量であるので機能は喪失しない.	影響なし.
		ϕ	破損箇所から, 圧縮空気が漏れておりシリンダの動作に影響がある場所の破損であるので，機能低下する.	P0 の要求動作を満たさないが，動作はする.
		0	破損箇所が大きい又は機能喪失する部分の破損であるため, 機能喪失する. 破損箇所が大きい場合は圧縮空気が大気に排出される.	圧縮空気が供給されないので P0 は出力しない.

付表 13　エアシリンダの FMEA（5/5）

部品名	故障モード	論理値	挙動	
			機　　器	P0　シリンダ出力
ヘッドカバー	亀裂	1	亀裂の大きさが小さいため亀裂部から空気が漏れるが影響はない.	影響なし.
		ϕ	亀裂の大きさが空気漏れを発生させる程度であるため, 圧縮空気排出量に影響がある.	P0 の要求動作を満たさないが，動作はする.
	固着	1	シリンダチューブに固着して取り外しができなくなっても, 機能には影響がない.	影響なし.
	詰まり	0	圧縮空気入力・出力ポートが詰まり圧縮空気が供給・排出できない.	圧縮空気供給されないので P0 は出力しない.