Specific Research Reports of the National Institute
of Industrial Safety, NIIS-SRR-NO.26 (2002)
UDC 338.312, 331.461: 62-192: 62-531: 62-781: 65.011.56

9. 稼動率に配慮した安全制御システムの構築法に関する基礎的考察*

梅崎重夫**，清水尚憲**

9. The Basic Study on the Constitution Method of the Safety Control System Considering the Coexistence of Availability and Safety*

by Shigeo UMEZAKI** and Shoken SHIMIZU**

***Abstract*:** The coexistence of availability and safety is a very important problem in the field of the industrial safety. However, the availability is sometimes decreased by improving safety when a trade-off model is established in the relation between safety and availability. The self developing spiral model was proposed for replacing the conventional trade-off model.

Two types of spiral models were examined in this study. The first model has no priority between safety and availability (described in Fig.2). Accidents might be occured when the initial safety level was not sufficient. On the other hands, the second model put the priority in safety (described in Fig.3). The possibility of accident occurence was very small because the complete safety measures were carried out before the operattion start.

Folowing results were obtained from the consideration of new spiral model.

(1) The fully safety measure such as the application of safety confirmation system is required in this model. The availability decreases because the machine stops frequently for ensuring safety of the operator. However, the drastic improvement in availability can be possible by clarifying and eleminating causes of machine stops. The availability is improved from 93% to 99.8% in a real automated product line.

(2) The application range of the dependability concept is examined in this study, and it is proved that this concept is limited to the system which can not sufficiently reduce the risk to the acceptable level in the design stage.

(3) There are two types of methods for improving availability, that is, the space-depend-type and the time-depend-type. Though the former can drastically improve the availability, the certainty is not enough. On the other hands, the latter is a reverse type for improving availability.

***Keywords*;** Industrial machinery, Safety, Safety control, Availability, Dependability

---

* 本研究の基礎となる部分は，第 28 回安全工学シンポジウム（平成 10 年 7 月 2 日）などに発表した。また，日本信頼性学会誌に投稿中である。

** 機械システム安全研究グループ　Mechanical and System Safety Research Group

1. はじめに

人間機械システムの災害防止対策では，機械の停止によって作業者の安全を確保する。しかし，大規模で複雑なシステムでは，たった一台の機械の停止によって稼動率が著しく低下することもある。このため，実際の現場では，稼動率に配慮した安全制御システム[1]の研究が様々な観点から進められてきた。

この具体例に，化学製品製造業であるA社の取り組みがある（後述する**Fig. 9** 参照）[2]。これは，安全方策によって発生する機械の停止を契機として抜本的な設備対策を実施し，稼動率を顕著に改善させた例である。また，輸送用機械器具製造業であるB社は，人間に対して直ちに危害を及ぼすおそれのある機械だけに停止を限定し，稼動率の大幅な改善を図ったとされている（後述する**Table 3** 参照）。これらは約 10 年近く前の事例であるが，現在にも通用する普遍性を持つ。

本報では，これらの取り組みの背後にある現場の知恵の理論化を図る。この分析を基に，稼動率に配慮した安全制御システムの最適設計手順の解明を目指す。また，以上の過程で，最近「信頼性・安全性」の分野で話題となっているディペンダビリティ概念（補足 1 参照）の産業安全分野への拡張可能性についても検討したので，併せて報告する。

なお，以上の議論では安全性を**Table 1** に示す指標[2),3)]で評価した。表で，非対称及び非対称誤りの正確な意味は文献 2）を参照されたい。また，「稼動率」は JISZ8115 で「アベイラビリティ」と呼ぶことになっているが，本報では現場の知恵の理論化が目的であるため現場で広く利用されている「稼動率」を用いた。

Table 1　The evaluation index of safety.
安全性の評価指標

区　分	指　標	意　味
確定的な安全方策	非対称誤り特性	安全側に誤る故障の頻度が危険側に誤る故障の頻度よりも著しく高い値を有する特性。または，安全側にしか故障しない特性。
非確定的なリスク低減策	非対称誤り率（回／回）	発生するすべての故障のうち，危険側となる故障の比率
	災害発生率（回／h）	単位時間あたりの災害発生率

注）表で，安全側とは機械が停止する側をいい，危険側とは機械が止まらなくなる側をいう。

2. 安全性と稼動率の両立モデル

これまで，安全性を決定するメカニズムは，稼動率とのバランスで妥協点を探るものであった。これは，概念的には**Fig. 1** のトレードオフ・モデルで表現できる。しかし，このモデルで決定される安全性は，立場の弱い作業者が不利となる均衡点に落ち着くこともある。また，このモデルでは安全性を向上させると，その影響で稼動率が低下する。

このため，最近では，安全性の向上が稼動率の改善をもたらし，この稼動率の改善が更なる安全性の向上をもたらすようにして，上述した問題点の解消を図るモデルも提案されている（たとえば，労働安全衛生マネージメントシステムの例など）。これはスパイラル・モデル[3]と呼ばれるもので，**Fig. 2** の自己発展モデルで表現できる。

この自己発展のループを無限に昇って行くことで，安全性と稼動率が極限まで向上した理想的な生産システムの構築が可能とされている。しかし，現実の人間機械システムでは，設備の運用開始までに適切な安全方策を実施しておかないと，自己発展の過程で災害が発生するおそれがある。

このため，本報では，設備の運用開始前までに徹底した安全方策を実施し，災害の発生を確実に防止した後に，スパイラル的に稼動率を改善させて行くモデルの検討を試みた（**Fig. 3** 参照）。以後，このモデルを安全性に優先順位を置いた自己発展モデルと呼ぶ。

このモデルは，安全方策の実施によって稼動率が低下するため，実用的でないとの批判がある。これに対し，筆者らは，徹底した安全方策は一時的な稼動率の低下を招くものの，この段階で抜本的な設備対策を講じれば，最終的には飛躍的な稼動率の改善を図れると考えた。以下，この考え方に基づく安全制御システムの構築可能性について順を追って検討する。

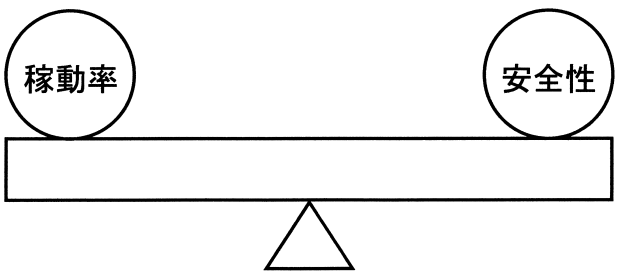
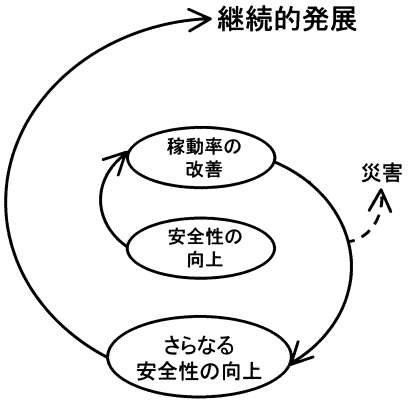
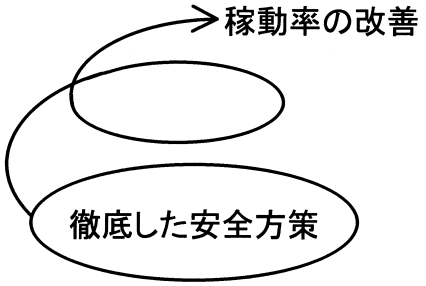


Fig. 1　Trade-off model.
トレードオフモデル



安全性と稼動率が相互作用によって
自己発展する「仕組み」

Fig. 2 Self developing spiral model.
自己発展モデル



徹底した安全性の向上が継続的な
稼動率の改善を生む「仕組み」

Fig. 3 Self developing spiral model which put the priority in safety.
安全性に優先順位を置いた自己発展モデル

3. 安全方策の例（安全確認システム）

本章では，**Fig. 3** のモデルに記載した「徹底した安全方策」について検討する。このモデルでは，災害の発生を確実に防止できる安全方策が必要である。この方策として，筆者が提案するのが安全確認システム[7] である。これは，安全が確認できるときに限って機械の運転を許可し，安全が確認できなくなったときは直ちに機械を自動停止させる制御システムである。

Fig. 4 に，安全確認システムの基本構成を示す。図で $I(t)$ は運転命令ありのときを論理値 1，運転命令なしのときを論理値 0 とする 2 値論理変数である。同様に，$P(t)$ は作業者が危険領域内に進入していないときを論理値 1，進入しているときを論理値 0，$W(t)$ は運転許可のときを論理値 1，運転禁止のときを論理値 0 とする 2 値論理変数である。

また，S は作業者が危険領域内に進入していないことを確認するセンサーであり，G は運転命令 $I(t)$ とセンサーからの安全情報 $P(t)$ の両方が論理値 1 であるときに機械の運転許可信号 $W(t)$ を発生する論理積演算要素（インタロック）である。

以上のシステムでは，ISO/IEC ガイド51[8] の記載にしたがって，残存リスクを許容可能な範囲まで低

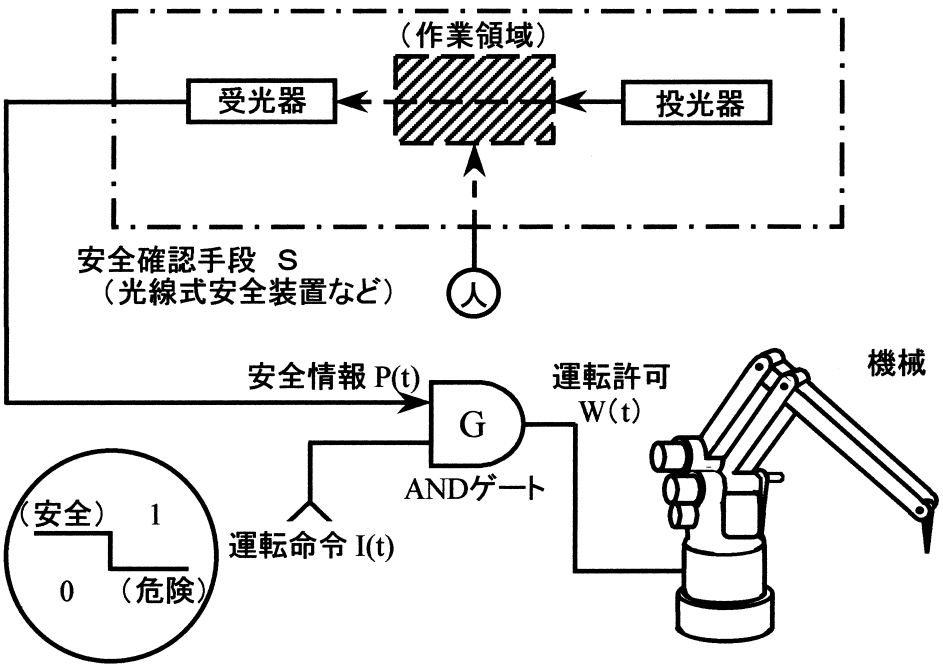


Fig. 4 Basic constitution of safety confirmation system.
安全確認システムの基本構成

減する必要がある。この許容可能なリスクの目標値として，筆者らは，文献４）で10^{-11}回／h 以下の災害発生率を設定した。**Table 2** に，この目標値を達成できる安全確認システムの構造要件を示す。なお，この要件に関する計算結果は文献４）を参照されたい。

4. 稼動率の改善策

4.1　自律分散形安全確認システムの導入

本章では，**Fig. 3** のモデルに記載した「稼動率の改善策」について検討する。安全確認システムでは，安全確保のためにすべての機械を停止させてしまうと，稼働率が低下して実用上の問題を生じる。そこで，人間に対して危害を及ぼすおそれのある機械だけに停止を限定する。このためには，個々の機械が独立したセンサーとインタロックを持ち，インタロックからの情報にしたがって自律的に機械を自動停止させるシステムを必要とする。

以後，これを自律分散形の安全確認システムと呼ぶ。これには，**Table 3** に示す従属形や独立形のモデルが考えられる。

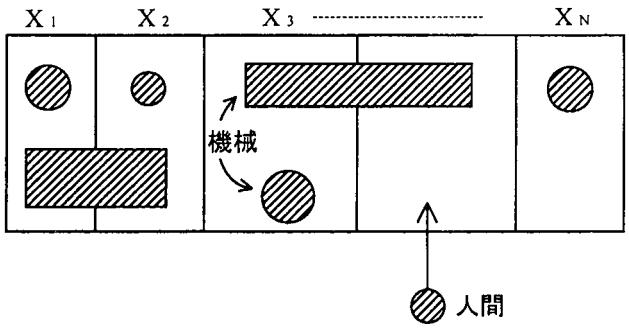
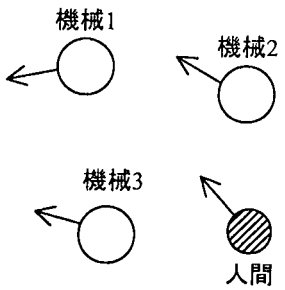
4.2　マルコフモデルによる稼動率改善策の定量化

自律分散形の安全確認システムは，人間機械システムの稼働率をある程度改善させる。しかし，前工程と後工程が密接に関連したシステムでは，たった一台の機械の停止によって稼動率が大幅に低下することがある。また，このシステムでは停止後の復帰操作に相当な手間を要することもある。

Table 2　The requirement for safety confirmation system which can achieve the desired value.
目標値を達成できる安全確認システムの構造要件

No	区　分		構造要件の例
1	センサー及びインタロックは	フェールセーフな安全確認形インタロック	一重系，10^{-5}h以内の自動監視，10^{-3}回／回の非対称誤り率
2		ハードワイヤードな制御装置	同種二重系，10^{-3}h以内の自動監視，10^{-1}回／回の非対称誤り率
3		プログラマブルな電子制御装置	異種三重系，0.5h以内の自動監視，1回／回の非対称誤り率

Table 3　Safety confirmation system of autonomous distributed type.
自律分散形安全確認システムの制御形態

（a）従属形	（b）独立形
	
作業者が進入した空間Xj内の機械を停止させる。 他の空間の機械は運転を継続させる。前工程と後工程の間に従属関係がある。	作業者に接近した機械だけを停止させ，他の機械は運転を継続させる。機械相互間が行う作業は独立の関係にある。

従来，このような場合の稼動率改善策は，現場担当者の勘や経験に依存していた。しかし，複雑なシステムになると，このような対応は明らかに限界がある。そこで，本報では，人間機械システムの挙動を状態遷移図で表現することで，稼動率改善策を定量的に評価し，稼動率低下の原因となっている問題点を抽出できるようにした。以後，時刻 t の瞬間にシステムが使用できる状態にある確率を瞬間稼働率（厳密には「瞬間アベイラビリティ」という。JISZ8115 参照）[9] といい，十分長い時間を経過した後の稼働率を定常稼働率（厳密には「定常アベイラビリティ」という。JISZ8115 参照）[9] と呼ぶ。

また，この検討では，安全性に関しても定量的な評価指標を導入する必要がある。しかし，確定的な安全方策は **Table 1** に示すように非対称誤り特性[7] で評価されるため，その定量化が図れない。そこで，非確定的な災害防止対策の評価指標である非対称誤り率[4] η を安全性の評価指標として導入した。この場合，確定的な安全方策は $\eta = 0$ なる特異点に繰り込むことができる。

Fig. 5 (a) は，この検討を行うための人間機械システムのモデルである。**Fig. 5** (a) で，P_O はシステムが正常状態にある確率で，P_H と P_S はシステムが異常状態にある確率を意味する。ただし，P_S はシステムが異常状態となったときに安全側（機械が停止する側）となる確率を，P_H はシステムが異常状態となったときに危険側（機械が暴走する側）となる確率を意味する。また，P_A は災害の発生確率である。

Table 4 に，**Fig. 5** (a) に記載された評価指標の意味を示す。ここで，**Fig. 5** (a) のモデルは，P_S と P_H に対しては修復系を，P_A に対しては非修復系を構成すると仮定する（補足 2 参照）。なお，本報では **Fig. 5** (a) のモデルを使った数値計算の簡素化を図るために，$H_L \ll 1$ であることを考慮し，その近似モデルとして **Fig. 5** (b) のモデルを用いた。これより，時刻 t における各確率の関係は次式となる[9]。

$$(dP_O/dt) = -\lambda P_O(t) + \mu_H P_H(t) + \mu_S P_S(t) \quad (1)$$

$$(dP_H/dt) = \lambda \eta P_O(t) - \mu_H P_H(t) \quad (2)$$

$$(dP_A/dt) = \lambda \eta H_L P_O(t) \quad (3)$$

$$(dP_S/dt) = \lambda (1-\eta) P_O(t) - \mu_S P_S(t) \quad (4)$$

ただし，初期条件として $P_O(0) = 1$，$P_S(0) = 0$，$P_H(0) = 0$，$P_A(0) = 0$ とする。

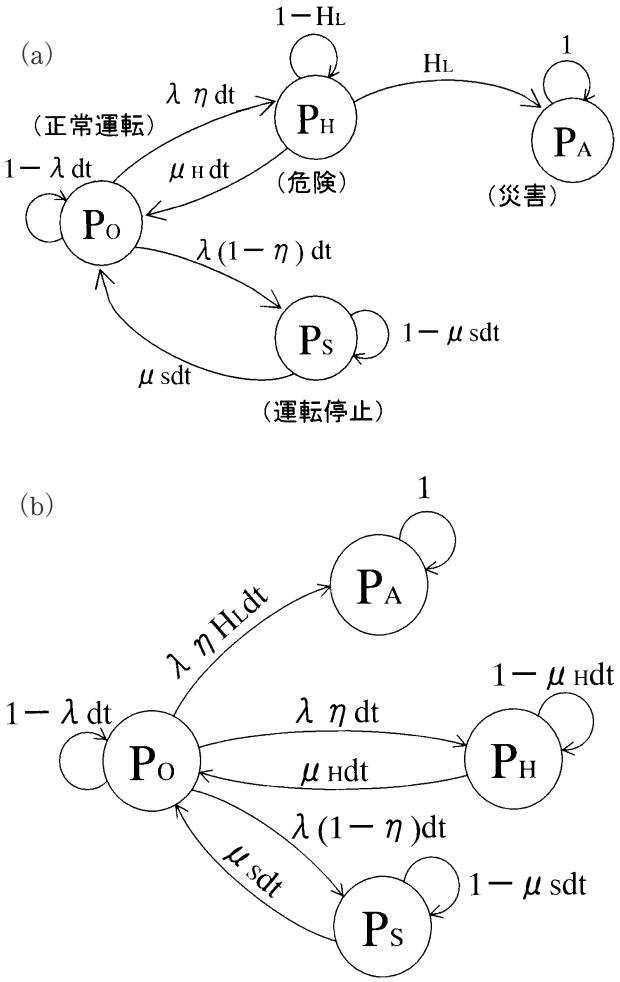


Fig. 5　State transition of man-machine system.
人間機械システムの状態遷移図

Table 4　The meaning of the evaluation index.
図に記載された評価指標の意味

記号	名　称	説　明
λ	トラブル発生確率（回／h）	人間の誤りや機械の故障などのトラブルに起因して，単位時間あたりにシステムが異常状態となる確率。
η	非対称誤り率（回／回）	発生するすべての故障に対する危険側となる故障の比率
μ	修復率（回／h）	単位時間あたりにシステムが修復する確率
H_L	回避失敗率（回／回）	システムが危険状態となったときに回避に失敗して災害となる比率
ε	早期異常検出率（回／回）	機械停止に至るおそれのある故障のうち，早期に検出できたために実際に機械停止を回避できた故障の比率

Fig. 5（a）のモデルでは，ISO/IECガイド51の記載にしたがって，残存リスクを許容可能な範囲まで低減する必要がある。この許容可能なリスクの目標値が，文献4）で示した10^{-11}回／h以下の災害発生率であることは既に述べた。これは，等価的には**Fig. 5**（a）で$\eta = 0$とすることに相当する。これより，**Fig. 5**（a）のモデルは**Fig. 6** のように変更できる。

Fig. 6 のモデルには，安全性に関連するパラメータが含まれていない。このことは，残存リスクを許容可能な範囲まで低減できるシステムでは，安全性と稼動率を個別に検討できることを示している。これは，また**Fig. 3** のモデルが現実のシステムとして実現可能であることを意味する。

以上より，時刻 t における瞬間稼働率$Av(t) = 100Po(t)$は次式となる[9]。

$$Av(t) = 100\mu s/(\mu s + \lambda)] + 100[\lambda/(\mu s + \lambda)]\exp[-(\mu s + \lambda)t] \quad (5)$$

4.3　修復率と故障率の改善による効果

（5）式は，人間機械システムの稼働率改善策に，次の 2 種類があることを示している。第 1 は，修復率μsの増大である。これは，機械が停止したときは直ちに作業者が駆けつけてトラブル処理を行った後，機械を再起動させるという方法である。

この方法は人間の柔軟な対応能力に依存することから，比較的容易に稼働率が改善できるという利点がある。しかし，人間に依存するために信頼性に乏しく，修復率もばらつきが大きい。したがって，この対策は他に方法がないときの最後の手段として選択すべきと考える。

第 2 の方法は，故障率λの減少である。この方法は，通常は相当な時間とコストがかかる設備対策を必要とする。したがって，この方式を採用した場合，対策を始めた当初の稼働率はむしろ低下する。しかし，一定期間を経て設備対策が完了した後は，従来以上の稼働率の改善を図れると推察される。

Fig. 7 は，以上の推察を定量的に確認するため，故障率λと修復率μsをパラメータとしたときの人間機械システムの定常稼働率Avを後述の条件の下で計算した例である。いま，この図で，システムが停止に至る毎にその原因と設備対策を徹底追及すると，復旧に要する時間が増大するため，等価的には修復率が減少する。これは，図の上では，設備対策当初の稼働率の低下として表れる。

この例で，停止後の復旧作業を平均して 5 分で完了できるものと仮定し，設備対策の検討に毎回平均して 30 分の停止が必要になったと仮定すると，修復率μsは 12 回／hから 2 回／hになるから，$\lambda = 1$回／hのときの定常稼働率は 92 %から 67 %へと大幅に低下する（**Fig. 7** の ① → ② 参照）。

これは生産管理上重大な問題となるが，この状態で数ヶ月を経た後に設備対策が効果を上げ始めると，稼働率は一転して急上昇を始める。これは，故障率λが減少するとともに，修復率が元に戻るためと考えられる。

この例で，設備対策が完了した後は，システムは 100 時間に 1 回程度の停止しか起こらないようになると仮定し，この修復に要する時間を 5 分と仮定すると，$\lambda = 0.01$回／h，$\mu s = 12$ 回／hとなるから，

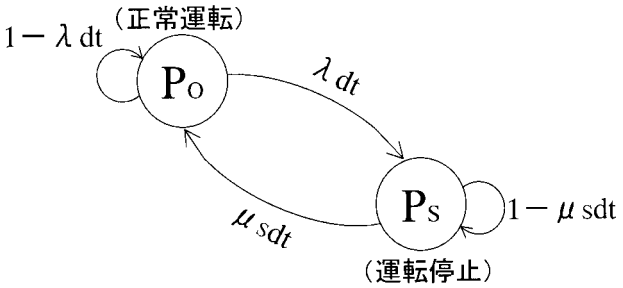


Fig. 6　State transition after the executing of safe measures.
安全方策を実施した後の状態遷移図

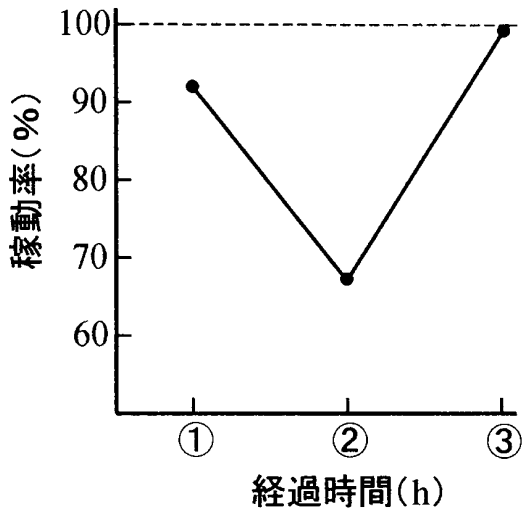


Fig. 7　Effectiveness improved by probability of trouble occurrence.
トラブル発生確率の改善による効果

定常稼働率は 99.9 %となる。これは，**Fig. 7** の ② から ③ に定常稼働率が向上したことに相当する。

4.4 早期異常検出率の改善による効果

以上の議論は，故障率の改善によって，稼働率を相当な水準まで改善できることを示している。しかし，最近の生産システムでは「操業開始から終了までに機械停止が希にしか生じないこと」が要求されることもあり，単に故障率を改善しただけでは，この水準の達成は困難と考えられる。

そこで，本報では，稼働率の改善策として，既に述べた故障率の改善策以外に，機械停止に至る故障（またはその兆候）を早期に検出して回避する対策を提案した。これは，一般にフォールト・トレラント対策と呼ばれているものである。このときの評価指標として筆者らが提案するのが「早期異常検出率」である。これは，「機械停止に至るおそれのある故障のうち，早期に検出できたために実際には機械停止を回避できた故障の比率」と定義する。

早期異常検出率が対象とする状態は，次に示す2種類がある。第 1 は，故障が発生したときでも，機械の機能を低下させることなく運転を継続している状態である。以後，これをタイプⅠの運転継続状態と呼ぶ。たとえば，無人搬送車のシステムで，無人搬送車が進行方向に存在する作業者を発見し，これを排除するために警報を発しながら高速走行している状態は，これに該当する。

これに対し第 2 は，故障が発生したときは機械の機能を一部低下させてでも，運転を継続しようとしている状態である。以後，これをタイプⅡの運転継続状態と呼ぶ。たとえば，無人搬送車のシステムで，

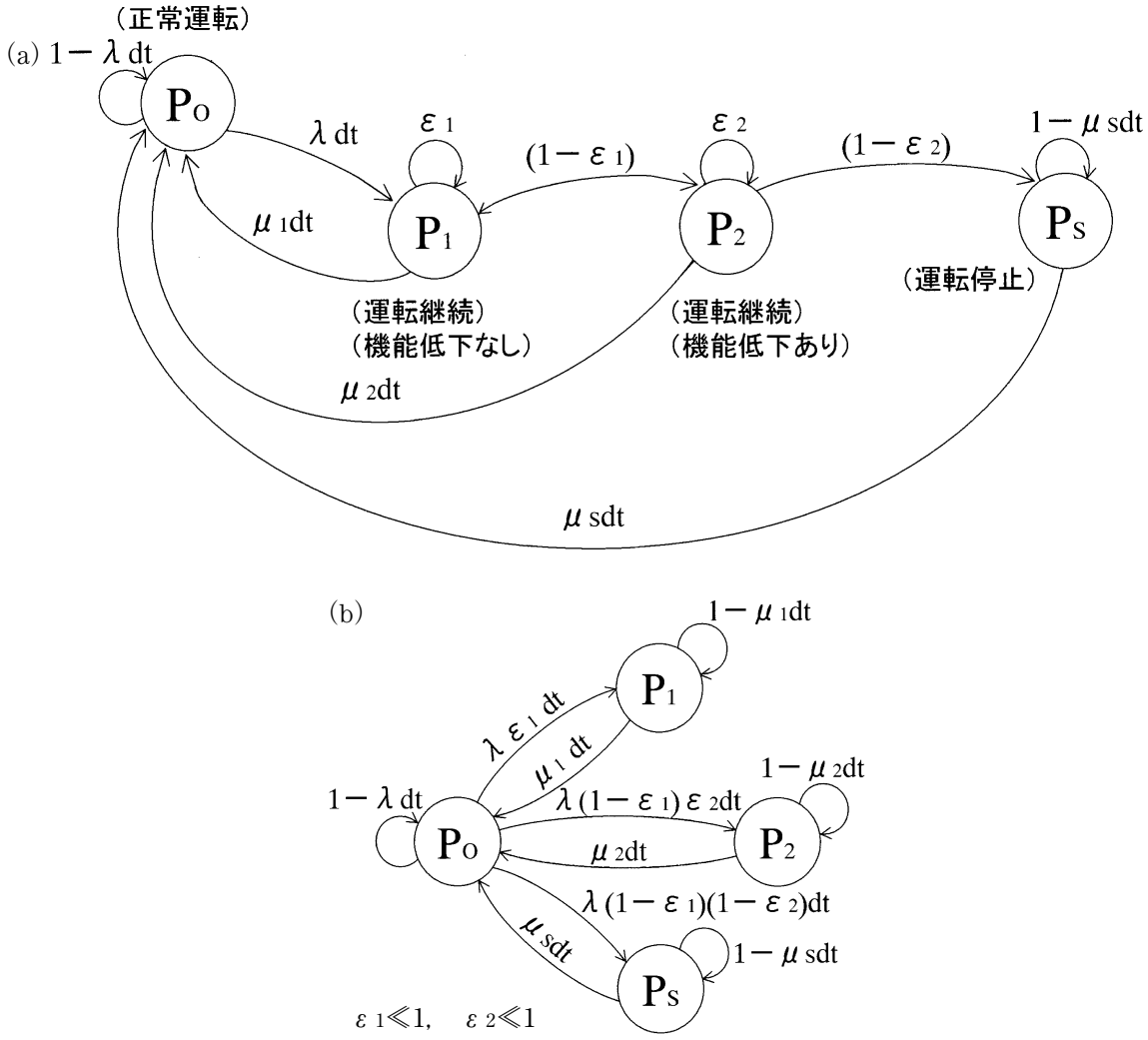


Fig. 8 State transition considering early detection rate of abnormal state.
早期異常検出率を考慮した状態遷移図

警報によっても人間が退去しないため，運転状態を高速から低速に切り替えてでも可能な限り運転を継続しようとする状態は，これに該当する。

Fig. 8 (a) は，早期異常検出率の改善効果を定量的に検討するためのモデルである。図で，P_0 はシステムが正常状態にある確率を，P_S はシステムが停止状態にある確率を意味する。また，P_1 は故障（またはその兆候）が発生したにもかかわらず機械がタイプⅠの運転継続状態にある確率を，P_2 は故障（またはその兆候）が発生したにもかかわらず機械がタイプⅡの運転継続状態にある確率を意味する。

さらに，タイプⅠに対応する状態の異常検出率を ε_1，タイプⅡに対応する状態の異常検出率を ε_2 とすると，早期異常検出率 δ は次式となる。

$$\delta = 1-(1-\varepsilon_1)(1-\varepsilon_2) = \varepsilon_1+\varepsilon_2-\varepsilon_1\varepsilon_2 \quad (6)$$

ここで，P_1に対する修復率を μ_1，P_2に対する修復率を μ_2，P_S に対する修復率を μ_Sとすると，時刻 t における各確率の関係は次式となる。なお，本報では **Fig. 8** (a) のモデルを使った数値計算の簡素化を図るために，$\varepsilon_1 \ll 1$，$\varepsilon_2 \ll 1$であることを考慮し，その近似モデルとして**Fig. 8** (b) のモデルを用いた。

$$P_0(t)+P_1(t)+P_2(t)+P_S(t)=1 \quad (7)$$

$$(dP_1/dt)=\lambda\varepsilon_1P_0(t)-\mu_1P_1(t) \quad (8)$$

$$(dP_2/dt)=\lambda\varepsilon_2\delta_1P_0(t)-\mu_2P_2(t) \quad (9)$$

$$(dP_S/dt)=\lambda\delta_1\delta_2P_0(t)-\mu_SP_S(t) \quad (10)$$

ただし，$\delta_1=(1-\varepsilon_1)$，$\delta_2=(1-\varepsilon_2)$ であり，初期条件として，$P_0(0)=1$，$P_1(0)=0$，$P_2(0)=0$，$P_S(0)=0$と仮定する。

(7) ～ (10) 式の一般解を求めるのは非常に困難である。そこで，時刻 $t \to \infty$としたときの定常解を求めると，確率 P_0に対応する定常稼働率 A_{0V}，確率 (P_0+P_1) に対応する定常稼働率$A1_{0V}$，確率 $(P_0+P_1+P_2)$ に対応する定常稼働率A_{2V}は，$\lambda=0.01$回／h，$\varepsilon_1=0.9$，$\varepsilon_2=0.99$，$\mu_1=120$ 回／h，$\mu_2=30$ 回／h，$\mu_S=1$ 回／hなる条件の下で 99.99 %以上となる（補足 3 参照）。

以上より，早期異常検出率の改善によって稼動率 99.99 %以上を達成できる可能性がある。これは，操業時間 1 万時間あたりの機械停止時間を1時間以下とする水準に相当する。これにより，「生産システムの操業開始から終了までに機械停止が希にしか生じないこと」が可能と推察される。

5. 検討結果

以上より，稼動率に配慮した安全制御システムの構築手順は次のようにまとめられる。

1）残存リスクを許容可能な範囲まで低減するために，安全確認システムを構築する。

2）稼動率改善のために，必要に応じて自律分散形の安全確認システムを構築する。

3）1）の対策を施した当初は，安全確保のために機械が頻繁に停止して稼働率は低下する。この場合の対応は従来は作業者に依存していた。

これに対し，本報で提案する対策では，設計者側が機械停止の原因を徹底的に追求して抜本的な設備対策を図る（故障率の改善）。これは相当なコストと時間を要するから，対策を始めた当初の稼働率は極端に低下する。しかし，一定期間を経て設備対策が完了した後は，従来以上の高い稼働率を実現できる。

4）実際のシステムでは「設備の操業開始から終了までに機械停止が希にしか生じないこと」が要求される。そこで，早期異常検出率の改善によって，3）で実現したよりも更に高い（たとえば 99.99 %以上）稼働率を実現する。

5）以上の対策によっても，希に機械は停止する。この場合の対応は人間に依存せざるを得ない。そこで，人間に教育・訓練を施すことによって機械停止後の修復率を改善し，稼働率の向上を図る。

6. 実施事例による実現可能性の検証

以上のうち，手順 3）以外は，現場での経験などから，その実現可能性が検証されている。これに対し，手順 3）に示した過程が実際に実現可能かは，検証されていない。そこで，本報では，化学製品製造業であるA社が，以上の考え方に基づいて自社の製造ラインに設備対策を施したときの稼動率変化を基に，手順 3）の実現可能性を検証した。

このラインは，10数台の機械が材料の挿入から製品（化粧品）に至るまでの一貫した加工と組立を行う自動生産ラインである。このうち，実験は，その中でも特にトラブルの多かった一台の成型機を対象とした。なお，実験の期間は 1994 年 4 月から 1995 年 5 月までの 13 ヶ月である。

Fig. 9[2] は，その実験結果である。図からも明らかなように，稼動率は 97 %から 88 %へと大幅に低下した後，一転して急上昇に転じ，最終的には99.8 %となった。これは，**Fig. 7** の概念図と一致する。なお，同社はこの曲線を信頼性分野におけるバスタブ曲線との比較で「キックオフ曲線」と呼んでいる。

実際の稼働率の改善過程は，次のような時間的経過をたどったと考えられる。

［A］作業者に対する安全方策として，システムの全

周囲を固定ガードで完全に囲った。ただし，トラブル処理や保全作業のために作業者がどうしても進入せざるを得ない箇所にだけは，可動ガードを設置した。このとき，作業者がカードを開いたときは直ちに機械が停止するように安全確認システムを構築した。

［B］ガードを設置したことにより，従来，作業者による臨機応変の措置によって覆い隠されていたトラブルは，可動ガードの開放による機械停止という形で明確に現れるようになった。

これに対し，当初，作業者からは「作業がやりにくい」，「機械が頻繁に停止して困る」などの苦情が 多発した。実際，対策を始める前の 11 月には 97 %であった稼働率は，対策開始直後の 12 月には 88 %まで低下した。

［C］このような事態に陥ったとき，普通の管理者は安全方策の継続を放棄してしまう。これに対し同社の管理者は，稼働率の低下は作業者がシステムを使いこなすようになるまでの一時的なものと判断し，将来の稼働率向上を期待して，対策の続行を決断した。

［D］以上のような経過をたどる中で，現場担当者の中からは稼働率を低下させるトラブル処理作業を減らすために抜本的対策を講じようとする機運が現れた。このため，現場ではトラブルの状況をコンピュータに取り込み，トラブルに至った理由を具体的に解明していった。その結果，従来考えていた問題点の他に，改めて多くのトラブル要因が判明した。そこでこれらも含めた設備対策を 1 月に完了した。

［E］当初の稼働率に戻るまで 4 ヶ月を要した。この期間はトラブルの顕在化とその対策及び改善の過程である。この過程では，従来，作業者が臨機応変に処理してきたトラブルの原因をシステムの欠陥と見なし，できる限り技術的な解決を図るようにした。

［F］以上の対策によって故障率が著しく減少したばかりでなく，作業者によるトラブル処理はガードを開き機械を停止しなければ出来ないようにしたので，安全性と稼動率が両立し，結果的に製造ラインのスピードを上げることもできた。現実には 30 %のスピートアップを行ったが，この経済的効果は大きいと考えられる。

7. 考察

7.1 ディペンダビリティの産業安全分野への拡張可能性

以上の議論は，ディペンダビリティ[10] の産業安全分野への拡張可能性の検討にも応用可能と考えられる。この概念は，既に IEC60050[11] で規定されており，元々信頼性または保全性技術として個別最適化されてきた固有技術をディペンダビリティという概念の導入によって全体最適を図ろうとする試みと筆者は考えている。

この前提には，「個別最適は必ずしも全体最適でない」という前提がある。言い換えれば，個別最適と全体最適が不一致であるような対象に，ディペンダビリティの概念は導入可能と考えられる。

検討の結果，確定的な安全方策では安全性と生産

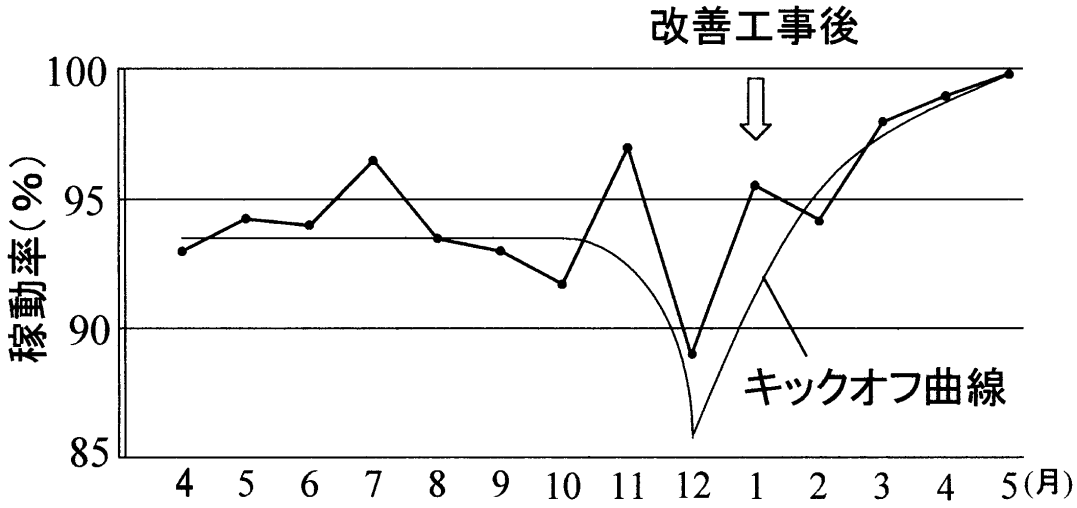


Fig. 9 Experimental result in the A company.
A社での実験結果

性の個別最適が全体最適になるために，ディペンダビリティの概念が適用される余地はない。一方，非確定的なリスク低減策では，安全性と生産性の個別最適が必ずしも全体最適にならない場合がある。これは残存リスクが許容可能なリスクの範囲内にない場合で，この場合にのみディペンダビリティの拡張可能性がある。

そこで，この場合の安全性の定量的評価指標として，既に文献4）で示した非対称誤り率[4]を提案する。また，ディペンダビリティの概念を産業安全分野へ拡張する際の基本モデルとして，以上の結果をまとめた **Fig. 10** に示す信頼性・安全性解析モデルを提案する。

7.2　本報で提案した稼動率改善策の効果

Fig. 9 に示したA社の事例は，運転可能な「時間」の拡張によって稼動率の改善を図るものである。この評価指標に時間稼動率[12]がある。これに対し，**Table 3** の事例（B社の事例に対応する）は，運転可能な「空間」の拡張によって稼動率の改善を図るが，この効果を適切に表現できる指標は見あたらない。

そこで，この指標として新たに空間稼動率Asを導入した。これは必ずしも一般的な概念ではないので，ここでは空間稼動率*As*%を「自律分散形を適用しないときと比較して機械が停止を免れる空間の割合」と仮に定義する（これは，稼動率というよりは厳密には「使用可能率」とでも表現した方が良いかもしれない）。これより，当初の稼動率Avは空間稼動率*As*の改善によって次式のAv'となる。

$$Av' = \frac{100A_V}{(100 - A_S)} \tag{11}$$

（11）式は，稼動率改善策に時間稼動率の改善と空間稼動率の改善という 2 種類のアプローチがあることを示している。

このうち，空間稼動率の改善は，稼動率を飛躍的に改善できる可能性がある。しかし，**Tablee 3** の従属形のように前工程と後工程が密接に関連したシステムでは，コンピュータ・シミュレーションを行っても稼動率の正確な計算は一般には困難である。また，**Table 3** の独立形のシステムでは，作業者の動きによってどの機械が停止するかはあらかじめ予想できない。これらは，稼動率改善策に不確定性を伴うことを意味する。したがって，空間稼動率の改善策は，あらかじめ稼動率に関する目標値を定め，この達成を必須とするシステムには適用が難しいと考えられる。

これに対し，時間稼動率の改善策では，故障率や早期異常検出率の改善などの抜本的な設備対策によって所定の目標値が達成できる可能性がある。

以上より，目標値の達成を必須とする場合の稼動率改善策は，故障率や早期異常検出率の改善などの抜本的な設備対策を中心とすべきことが判明した。これに対し，自律分散形を中心とした対策は，「（不確定であっても）結果的に稼動率が大幅改善できれば良い」とする場合に適する。したがって，これら両者の得失を勘案して，最適な稼動率改善策を選択すべきである。

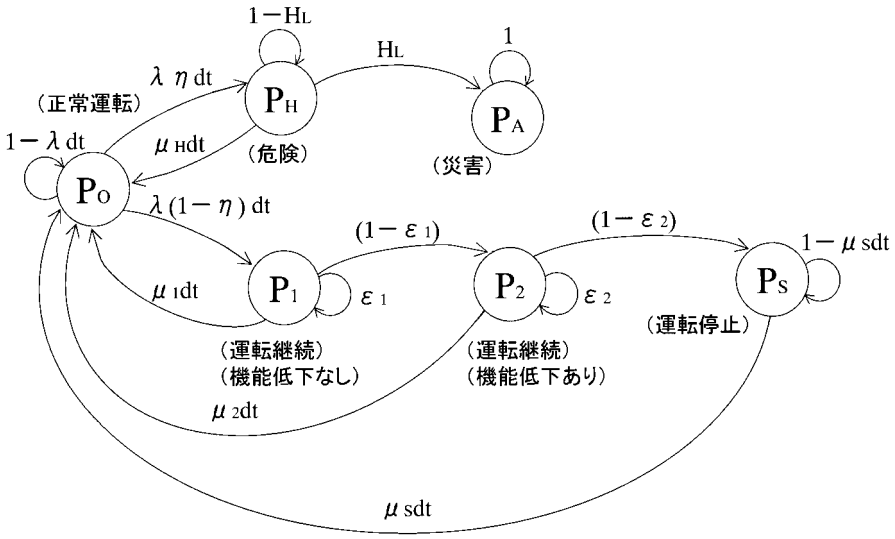


Fig. 10　The examination model of the dependability.
ディペンダビリティの検討モデル

8. おわりに

以上，稼動率に配慮した安全制御システムの構築法について検討した。これによって得られた結果は，次の通りである。

1）稼動率に配慮した安全制御システムは，安全性に優先順位を置いた自己発展モデルに基づき構築可能である。これは，従来考えられてきたトレードオフモデルとは，明確に異なる。

2）上記のモデルでは，安全方策によって発生する機械の停止を契機として抜本的な設備対策を実施し，稼動率を顕著に改善できるという理論が事例によって確認された。

3）ディペンダビリティの概念は，非確定的なリスク低減策のうち設計段階で許容可能なレベルまで残存リスクを低減できないものに限って産業安全分野にまで拡張可能性がある。

4）稼動率改善策には，空間稼動率と時間稼動率の2種類のアプローチがあり，この両者の得失を考慮した使い分けが必要である。

謝　辞

本研究は，北九州市立大学国際環境工学部 杉本旭教授と中央労働災害防止協会 粂川壮一氏の指導の下で実現したものである。適切な御指導を頂いた両氏と，貴重なデータを提供して頂いたA社の関係諸氏に深い感謝の意を表する。

参考文献

1）梅崎・杉本・粂川，生産性に配慮した安全制御システムの検討，日本機械学会第 7 回交通物流部門大会講演論文集（1998）pp.433-436.

2）向殿ほか，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（2001）pp.190-193.

3）坂崎・雫・田邊・豊田他，ISO安全・品質・環境早わかり，日本規格協会（1997）p.150.

4）梅崎・杉本・中村，産業機械の安全方策に関する基礎的考察－リスク評価に含まれる不確定性を考慮した安全方策の提案－，日本信頼性学会誌，Vol.23，No.7（2001）pp.659-675.

5）JISZ8141, 生産管理用語（基本），JISハンドブック品質管理（2001）p.171.

6）産業安全研究所特別研究報告（生産・施工システムの総合的安全制御技術の開発に関する研究，第 3 報：大規模生産システムを対象とした安全制御技術の開発），NIIS-SRR-NO24（2002）pp.71-76.

7）工作機械等の制御機構のフェールセーフ化に関する指針（案）の解説，日本労働安全衛生コンサルタント会（1997）pp.4-7.

8）Revision of ISO/IECガイド51, Safety aspct-Guidelines for their inclusion standards（1997）.

9）川崎，信頼性設計，日科技連（1985）p.149.

10）JISZ8115，ディペンダビリティ（信頼性）用語，JISハンドブック品質管理（2001）p.88.

11）IEC60050, Dependability and quality of service Part1: Dependability common terms.

12）鈴木他，生産革新のための新TPM展開プログラム，日本プラントメインテナンス協会（1995）p.29.

13）杉本・蓬原，安全の原理，機械学会論文誌，C編，56-530（1990）pp.2601-2609.

［補足1］

ディペンダビリティとは，「アベイラビリティ性能及びこれに影響を与える要因，すなわち信頼性性能，保全性性能及び保全支援能力を記述する包括的な用語。非定量的用語として一般的記述に限り用いられる」[1)]と定義される。

国際規格では「ディペンダビリティの概念を安全分野にまで拡張すべきでない」としているが，リスク解析は可としている。そこで，本研究では，リスクの解析と評価に限って，ディペンダビリティの概念を産業安全の分野まで拡張することにした。

［補足2］

これは，安全側故障では機械が停止するために容易に検出できるのに対して，危険側故障では機械が停止できなくなるために容易に検出できないためである。

［補足3］

このときの計算式は，次式で与えられる。

$$A_{0V} = (1 / C_1) \quad \text{(A1)}$$

$$A_{1V} = (C_2 / C_1) \quad \text{(A2)}$$

$$A_{2V} = (C_3 / C_1) \quad \text{(A3)}$$

ただし，

$$C_1 = 1 + \rho_1 \varepsilon_1 + \rho_2 \delta_1 \varepsilon_2 + \rho_S \delta_1 \delta_2$$

$$C_2 = 1 + \rho_1 \varepsilon_1$$

$$C_3 = 1 + \rho_1 \varepsilon_1 + \rho_2 \delta_1$$

$$\rho_1 = \lambda / \mu_1$$

$$\rho_2 = \lambda / \mu_2$$

$$\rho_3 = \lambda / \mu_S$$

（平成 14 年 8 月 9 日受理）