Specific Research Reports of the National Institute
of Industrial Safety, NIIS-SRR-NO.24 (2002)
UDC 331.461:62-192:62-531:62-781:65.011.56

6. 広大領域内の安全確認を目的とした複数作業者用安全確認システムの開発と評価*

梅崎重夫**

6. The Development and Evaluation of the Safe Confirmation System for Many Operators Cooperating in Large Scale Working Areas*

by Shigeo UMEZAKI**

Abstract: This report proposes a new safety system for counting the number of operators in the moving area of the machine. It was very difficult to create such a system because the operator could enter into the machine moving area without pulling out of the interlocking key, and there were not only nominated operators but also non-nominated operators, passers-by, or observers in the actual field. Therefore, the system which can recognize the presence position of operators by the movement of interlocking keys was developed in this study.

This system had next features:

(1) The behavior of the operator was devided into 3 types, that is normal action, hazardous side error and safe side error. The hazardous side error means that the machine can not stop in spite of the presence of the operator in the machine moving area. For example, it arised when the operator did not extract the interlocking key as he entered into this area. In order to prevent such an error, the machine operation should be permited only when the certain action pattern of the operator (the order of pulling the interlocking key, stepping safety mat switches. etc.) was normal.

On the other hand, the safe side error means that the machine stops in spite of the absence of the operator in the machine moving area. For example, it arised when the operator did not extract the interlocking key as he went out from this area. The restart of the machine was required in this case because the safety problem caused.

The optimum safe confirmation systems corresponding to each case were developed in this study.

(2) The system considering not only nominated operators but also the behavior of the work director, non-nominated operators, passers-by or observers was developed. The restart system for the work director was also developed in this study.

(3) The fail-safe system was realized by the programmable logic controller with triple redundancy, diversity and the self checking mechanism. The memory checking function was also very important for this system.

Keywords; Safety control, Fail-safe, Diversity, Redundancy, Self checking, Programable controller, Safe confirmation, Human detection system

---

* 本研究の一部は，第 17 回日本ロボット学会学術講演会（平成 11 年 9 月 9 日）で発表した。
** 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

大規模生産システムでは，複数の作業者が安全確保領域内に進入するときの対策として，キースイッチを設ける場合が多い。しかし，キーによる対策では，作業者がキーを抜かないで安全確保領域（補足1参照）に進入すると，当該領域内に作業者が存在しているにもかかわらず，誤って「存在していない」と判断されて，機械が運転を開始してしまうことがある。

このため，筆者らは，このような事態が生じないように，安全確保領域の進入箇所に監視装置（マットスイッチや光線式安全装置など）を設け，作業者によるキー操作及び安全確保領域への進入行動が一定の時間的・空間的条件を満足しているときに限って機械の運転を許可する安全確認システム[1)]を検討してきた。しかし，このシステムの制御は，対称誤り特性[1)]（補足2参照）を持つプログラマブル・コントローラ（以下「PLC」と略記する）に頼るしかなかったために，フェールセーフな安全確認システムの構築は不可能と考えていた。

これに対し，最近，欧州で異種冗長化（異なった種類のCPUによる冗長化）された3種類のPLCの演算結果がすべて同一であるときに限って機械の運転許可信号をオンとするという汎用安全コントローラ[2)]が開発された。このコントローラは既に第2編で述べた通り，きわめて高い非対称誤り特性[1)]を持つ。したがって，このコントローラを応用すれば，フェールセーフな安全確認システムの構築が可能と考えられる。

そこで，本研究では，このコントローラを応用して，大規模生産システムを対象としたフェールセーフな安全確認システムの開発を試みた。

2. 安全確認の条件

いま，**Fig. 1** のように大規模生産システムの安全確保領域を Xで表し，領域 X以外の任意の領域を Yとする。ただし，Yは大型工作機械（占有領域がある程度広いものであれば，特に限定しない）から十分離れているために，作業者が労働災害を被らないことが確認されている領域とする。

また，領域 Xと Yで作業を行う指名を受けた作業者を記号 $H_0, H_1, \cdots, H_N$で表し，H_0を作業主任者，$H_1, \cdots, H_N$を作業主任者の指揮監督を受けて作業を行う一般作業者とする。さらに，一般作業者以外の第三者を記号 $H_N+1, \cdots, H_\infty$で表す。ただし，第三者には指名作業者以外の作業者や通行人，見学者などが含まれる。

ここで，時刻 t において領域 Xに作業者または第三者 H_J $(J = 0, 1, 2, \cdots \infty)$ が存在していないことを $\overline{H_J(x,t)} = 1$，存在していることを $\overline{H_J(x,t)} = 0$ で表し，時刻 t において領域 Yに作業者または第三者 $H_J(J = 0, 1, 2, \cdots \infty)$ が存在していることを $H_J(y,t) = 1$，存在していないことを $H_J(y,t) = 0$ で表す。ただし，$\overline{H_J(x,t)}$ は存在していないときを論理値1，存在しているときを論理値0とする2値論理変数である。また，$H_J(y,t)$ は存在してるときを論理値1，存在していないときを論理値0とする2値論理変数である。

このとき，災害が発生しないためには，領域 Xに作業者または第三者が一人も存在していないか，または，領域 Yにすべての作業者および第三者が存在していることが条件となる。

この関係は，次式で表すことができる。

$$\prod_{J=0}^{\infty} \overline{H_J(x,t)} = 1 \quad \text{または} \quad \prod_{J=0}^{\infty} H_J(y,t) = 1 \qquad (1)$$

実際の安全確認システムでは，広大な領域 X及び Yの全域を確認するのは不可能である。そこで，これに代わる方式として，**Fig. 1** に示すように領域 X内に内部キーボックス，領域 Y内に外部キーボックスを設け，作業者 $H_0, H_1, \cdots, H_N$に各々キー $K_0, K_1, \cdots, K_N$を割り当てる。

ここで，時刻 t において内部キーボックスにキー K_J $(J = 0, 1, 2, \cdots N)$ が差し込まれていないときを $\overline{I_J(t)} = 1$，差し込まれているときを $\overline{I_J(t)} = 0$ で表し，時刻 t において外部キーボックスにキー $K_J(J = 0, 1, 2, \cdots N)$ が差し込まれているときを $O_J(t) = 1$，差し込まれていないときを $O_J(t) = 0$ とすると，(1) 式は次式となる。

$$\prod_{J=0}^{N} \overline{I_J(t)} = 1 \quad \text{または} \quad \prod_{J=0}^{N} O_J(t) = 1 \qquad (2)$$

ただし，$\overline{I_J(t)}$ はキーが差し込まれていないときを論理値1，差し込まれているときを論理値0とする2値論理変数である。また，$O_J(t)$ はキーが差し込まれているときを論理値1，差し込まれていないときを論理値0とする2値論理変数である。

3. システムの基本構成

3.1 危険側誤りと安全側誤り

(2) 式では次のような点が問題となる。

① 作業者はキーを抜かないで領域 Xに進入したり，二人以上の作業者がキーを一個だけ抜いて同時に領域 Xに進入するかもしれない。この場合，作業者とキーの間に一対一の対応関係が成り立たない。

② 第三者とキーの間には，まったく対応関係がない。

いま，この問題を一般的に議論するために，領域 X 内に存在する作業者の数を N_H，内部キーボックスに差し込まれたキーの数を N_K とすると，これらの間には，少なくとも次の 3 種類の関係が考えられる。

(a) $N_H = N_K$ の場合（正常）

これは，作業者とキーの間が一対一の対応関係を保って領域 X への出入りを行っている場合である。

(b) $N_H > N_K$ の場合（危険側誤り）

これは，作業者がキーを抜かないで領域 X だけ抜いて同時に領域 X へ進入したり，一人に進入したり，二人以上の作業者がキーを一個の作業者がキーを二個以上抜いて領域 X から退出する場合などに発生する。この場合，領域 X 内に作業者が存在しているにもかかわらず，誤って「存在していない」と判断されて，機械が運転を開始してしまう。以後，これを「危険側誤り」と呼ぶ。

(c) $N_H < N_K$ の場合（安全側誤り）

これは，作業者がキーを抜かないで安全確保領域から退出したり，二人以上の作業者がキーを一個だけ抜いて同時に領域 X から退出したり，一人の作業者がキーを二個以上抜いて領域 X に進入する場合などに発生する。この場合，領域 X 内に作業者が存在していないにもかかわらず，誤って「存在している」と判断されて，機械が停止したままの状態となる。以後，これを「安全側誤り」と呼ぶ。

3.2 危険側誤りに対するシステム

以上のうち，安全上問題となるのは (b) の危険側誤りである。そこで，本研究では，次の点に注目して危険側誤りに対するシステムを構成した。

[A] 作業者が「外部キーボックスからキーを抜く」→「一定時間内に **Fig. 1** のマットスイッチを α, β, γ の順序で踏む」→「一定時間内に作業者が対応する内部キーボックスにキーを差し込む」という一連の行動が正常に行われたときに限って，作業者が安全確保領域の内部で行う操作によって機械の手動運転が出来るようにする。

[B] 作業者が「内部キーボックスからキーを抜く」→「一定時間内にマットスイッチを γ, β, α の順序で踏む」→「一定時間内に作業者が対応する外部キーボックスにキーを差し込む」という一連の行動が正常に行われたときに限って，作業者が安全確保領域の外部で行う操作によって機械の自動運転が

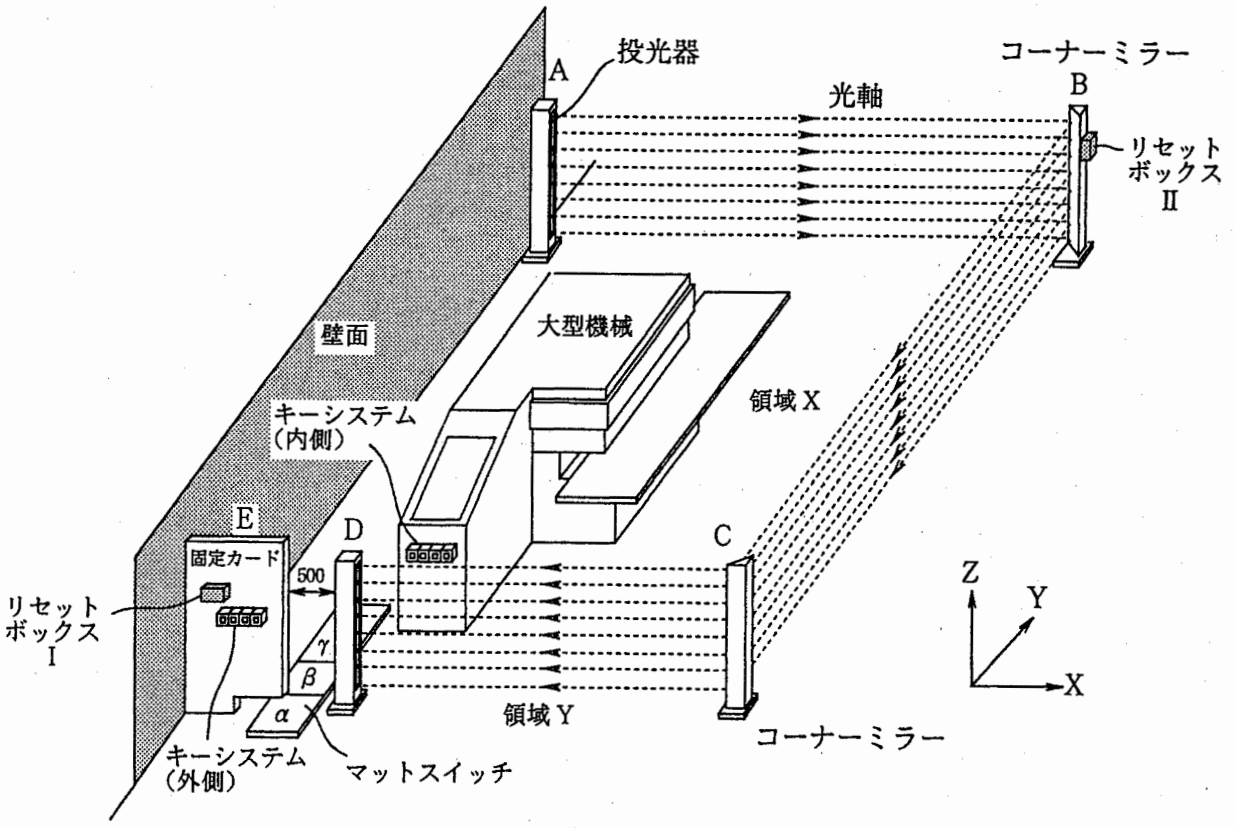

Fig. 1　The basic configuration of the safe confirmation system.
安全確認システムの基本構成

出来るようにする。

[C]　作業者が領域Xに出入りするのは，**Fig. 1** のD–E間とする。この幅は，二人以上の作業者が同時に安全確保領域に進入できないように500 mm以内とするとともに，一人しか乗れない400 mm正方のマットスイッチβを設ける。

[D]　外部キーボックスのキーを抜いても，一定時間（たとえば，10秒）以内でなければ作業者の進入は許可されないようにする。

[E]　安全確認システムの電源が切られた状態で作業者が領域Xに進入すると，作業者が領域X内に存在しているにもかかわらず，存在していないと判断する危険側誤りを生じる。そこで，機械の駆動用電源を遮断した後でも安全確認システムだけは通電が継続するようにしている。

また，万一安全確認システムの電源が遮断されたときは，特定のタグ（鍵）を持った作業指揮者（3.3節参照）によるリセット操作が行われない限り，システムが起動しないようにする。

3.3 安全側誤りに対するシステム

(c)の安全側誤りでは，機械が停止したままの状態を解除するために，安全確認システムのリセット操作を必要とする。しかし，この操作を一般の作業者に委ねると，せっかくの安全確認システムの効果がなくなる。そこで，本研究では，特定のタグ（鍵）を持った作業指揮者が，このタグによってだけ開けられるボックスを設け，このボックス内のスイッチを操作しなければリセットを行えないようにシステムを構成した。

このスイッチは，**Fig. 1** のIとIIの2カ所に設置し，一定時間以内にII→Iの順序でスイッチ操作を行わなければリセットと見なさないようにした。

4. システムの具体的構成

実験のため設定した安全確保領域Xは，**Fig. 1** のAB間で2.6m，BC間で6.9m，CD間で1.9m，DE間で0.6mであった。また，光線式安全装置はドイツ・ジック社製のFGS1800シリーズであり，防護高さ1800 mm，光軸間隔15 mm，連続遮光幅30 mmであった。この装置では，**Fig. 1** の投光器Aから発光した光は，コーナーミラー（鏡面反射板）B及びCで反射し，最終的に受光器Dに到達する。

キーボックス（外側及び内側）には，米国シグマ・コントローラ社のPROSAFE RKS10を使用した。これは，種類の異なるキーが4種類設置されており，外側と内側のキーボックスのキーが左右から順番に一対一対応している。

マットスイッチには，米国SG社のマットスイッチAFシリーズを使用した。このうち，マットスイッチαは900 mm×900 mm，マットスイッチβは300 mm×300 mm，マットスイッチγは900 mm×900 mmの寸法を有する。

フェールセーフな汎用安全コントローラには，ドイツ・ピルツ社製のPSS3100を使用した。このコントローラでは，異種のCPUを三重化しているために，三種類のCPUが同時にハードウェア故障を起こす可能性はきわめて少ない。また，各CPU上で処理されるソフトウェアも異なっているために，ソフトウェアのバグによって誤って運転許可信号が発生する可能性もきわめて少ない。さらに，CPUを使用したシステムでは，メモリの異常による誤動作が問題となるが，本システムでは個々のCPU毎に独立してメモリを持つとともに，自己診断装置によってシステムの始動時及び運用時に定期的に全メモリの同一性を確認している。以上のような構成によって，故障時に誤って運転許可信号を出力しないフェールセーフなシステムの実現を可能としている。

5. システムの総合評価と今後の課題

本研究では，（社）日本労働安全衛生コンサルタント会が実施した「フェールセーフ化促進委員会」の指導を受けながらシステム開発を行った。この委員会は，大学でフェールセーフ技術を研究している研究者，工作機械の設計技術者，及び機械設備のユーザーなどから構成されていた。

この検討過程で，当初，筆者は，各作業者毎に特定のキーをあらかじめ与えておき，これを安全確保領域内のキーボックスに差し込んだときに限って，機械の手動運転を許可する方式を提案した。しかし，この方式では，「作業者が一人でもキーをなくすと，機械が運転できない」，「作業者数が多くなると，キーの管理が大変」，「作業者が30人いるとして，30個もキーボックスを設置するのか」などの問題点が指摘された。このため，本研究では，次善の策として本報で記載した方式を提案した。しかし，現段階で評価すると，作業者数が数人の場合は，当初方式の方が適切であったと推察される。

また，委員会に参加した大学の研究者からは，「本研究の実施にあたっては，まず広大領域内で複数作業者が共同して作業を行う際の論理的関係を明らかにすべきである」との指摘を受けた。これに応じて検討したのが，第2章と第3章である。これについては，多少難解であるが，論理的関係を的確に表現しているとの評価を受けた。

さらに，他の大学の研究者からは「安全システムの制御電源を切った場合は，システムが有効でなくなる」との指摘を受けた。このため，本システムでは，機械の駆動用電源を遮断した後でも安全確認システムだけは通電が継続するようにしている。しかし，この構成では，停電や遮断器の作動などが起きたときは有効でない。そこで，バッテリーを予備電源とした警報システムを検討中である。

さらに，委員会に参加していた現場管理者からは,「作業全体を指揮する作業指揮者と，一般作業者の役割分担（権限）が明確になるようなシステム構成とすべきである」との指摘があった。この点に関しては，リセット権限の作業指揮者への限定という方策を講じているが，他の重要事項で見落としがあるかも知れない。

6. おわりに

特定領域内に進入または退出する人員を正確に数えるのは，技術的にはきわめて難しい課題とされている。また，実際の現場では，作業者だけでなく，第三者（指名作業者以外の作業者や通行人，見学者など）の進入も考慮する必要がある。このため，本研究では，指名作業者と一対一に対応するキーを設け，このキーの挙動をもって作業者の挙動を把握する安全確認システムを開発した。

このシステムは，次の特徴を持つ。

1) 大規模生産システムで発生する作業者の挙動を，正常，危険側誤り，安全側誤りの 3 種類に分けて，それぞれの場合に応じたシステムを構築した。
2) 指名された一般の作業者だけでなく，作業指揮者や第三者の挙動も考慮したシステムを構築した。
3) 異種冗長化と自動監視機能を備えた汎用安全コントローラを応用してフェールセーフな安全確認システムを実現した。

以上が本システムの概要であるが，本システムは既に第 5 章に示したように完全なものではない。また，システムの評価もきわめて多人数による長期的運用が不可欠であり，このような評価を完全に実施するには至っていない。今後は，第 5 章で示した本システムの高度化に取り組むとともに，開発したシステムを実際の現場に適用し，その有効性を評価するのが課題である。

参考文献

1) 労働省，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 (1998).
2) 三平律雄他，PSDI に何が起こっているか，プレス技術, Vol.35, No.10, (1997), pp.116–121.

[補足 1]

安全確保領域とは，機械の危険な可動部の動作に対して安全を確保すべき領域であり，機械の危険な可動部の動作領域や，安全隙間，安全距離等を考慮して設定した領域をいう。

[補足 2]

ここでいう対称誤り特性とは，システムに故障が発生したときに安全側（機械が止まる側）となるか危険側（機械が暴走したり，止まらなくなる側）となるか不確定なものをいう。具体的には，CPU を使った装置は一般に対称誤り特性を持つと言われている。

これに対し，非対称誤り特性とは，安全側となる頻度の方が危険側となる頻度よりも著しく高くなるか，または安全側にしか故障しない特性をいう。具体的には，フェールセーフなシステムが非対称誤り特性を持つと言われている。

安全に関連したシステムは，非対称誤り特性を持つものでなければならない。

(平成 14 年 1 月 10 日受理)