

2. 安全確認型と危険検出型

危険源をとり除く〔 $H=0$ 〕という手法は「安全状態」を作るために最も有効な手段ですが、生産現場は通常大きなエネルギーを使用して物づくりをしており、危険源を除去できるケースは限られます。そこで一般的には、危険源をカバーや柵で囲い込んで人を危険源から隔離して曝露を防ぐ手段（「1. 確定的安全と確率的安全」で述べた手段 d.）が用いられます。この場合、隔離した状態を常時保てればよいのですが、工程条件の変更など作業の都合上、隔離状態を解除して設備の可動部など危険源に接触する必要もあります。

このように隔離状態を解除して危険源に接触する場合に用いられる安全システムには次の二つがあります。

- ①危険検出型システム：人が危険源に曝露する危険な状態が生じてないか否かを確認（検知）して、危険な状態の証拠が確認された時にエネルギーの形で危険情報を出して設備の運転を停止させるシステム
- ②安全確認型システム：人が危険源から隔離された安全な状態にあるかどうかを確認（検知）して、安全な状態の証拠が確認された時だけエネルギーの形で安全情報を出して設備の運転を許可するとともに、安全状態が確認できなくなったら直ちに安全情報（エネルギー）を遮断して運転を停止させるシステム

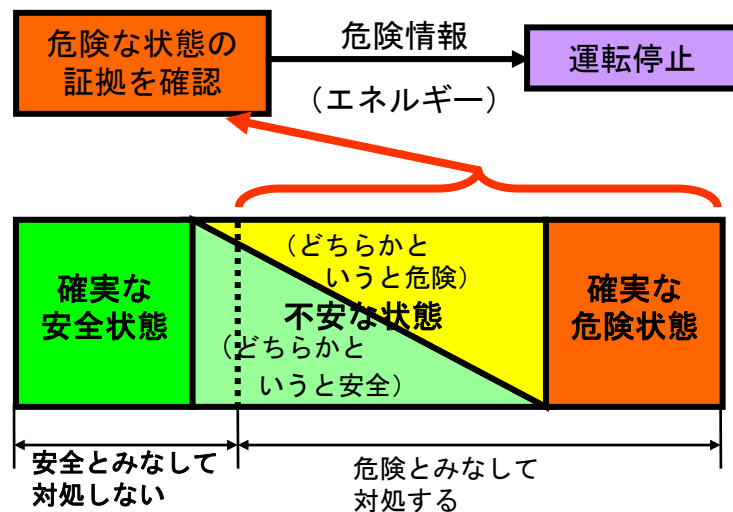


図2-1危険検出型

「危険検出型」の場合、検知手段、情報の伝達手段のいずれかが故障すると危険状態になっても設備を停止させるための危険情報（エネルギー）が伝わらず設備が停止できない（及び運転の停止手段が故障した場合も停止できない）という本質的な欠陥があります。そのため、検知手段、情報の伝達手段あるいは停止手段は、故障の少ない信頼性のあるものを使用するとともに、安全システムが故障していないかどうか点検を行うことが必要になります。それでも心配な場合は、システムを二重・三重にしたり、他の安全システムと組み合わせたりしますが、それでも故障確率をゼロにすることはできないので、安全の確保は確率的になります。

また、生産現場には、人が危険源に確実に暴露する状態（以下「**確実な危険状態**」と呼び

ます)、および、人が危険源に暴露する可能性がゼロの状態（以下「**確実な安全状態**」と呼びます）のほかに、特別なことをしない限り（特別なことが生じない限り）暴露する可能性が低い「どちらかという危険（あるいは、どちらかという安全）」という曖昧な状態（以下「**不安な状態**」と呼びます）が存在します。この不安な状態の危険源の全てについて危険検出型システムで対処できればよいのですが、数が多く、要する費用・時間を考えると現実的には不可能です。そのため、図 2-1 に示すように、不安な状態の一部に対処し得ない部分が残ることになります。この部分は、事故・災害が生じた時点で対処しているのが現実ですが、安全管理をしっかりとやっている企業で死亡・永久損失災害が発生するのはこの部分が多いのです（ここに安全対策上のジレンマがあります）。

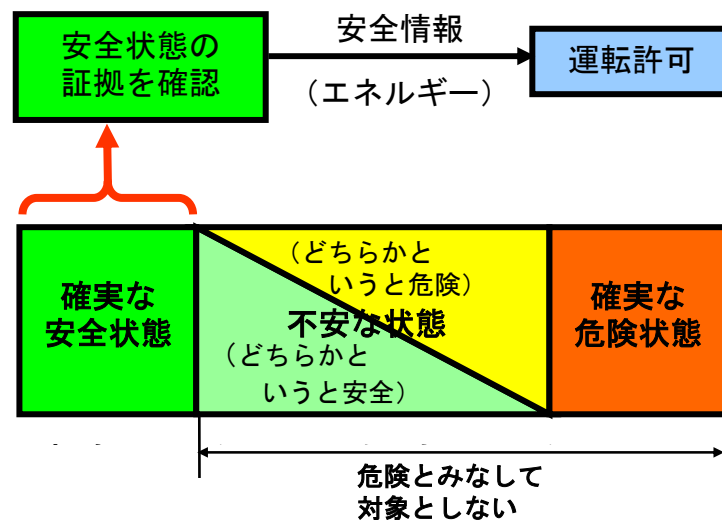


図2-2 安全確認型

これに対して「安全確認型」の場合は、「不安な状態」を「確実な危険状態」とみなして「確実な安全状態」だけを対象とします。そして「確実な安全状態」の証拠を確認（検知）した情報（エネルギー）を用いて設備の運転を許可・継続するので、検知手段や情報の伝達手段が故障して安全情報が伝わらなくなると設備へのエネルギー供給が遮断されて設備は自動的に停止します。そのため、停止すれば安全が確保できるシステムの場合は確定的に安全を確保できますし、予防保全やシステムの二重化などは不要です（故障すると設備が停止して稼働率が低下するので、生産性を確保するために予防保全や安全システムの二重化を行うことはあります）。

「『確定的』な手段を用いて常に『確実な安全状態』を維持する」、このことによって始めて、人が誤りを犯したり機械が故障しても安全が確保される「確定的安全状態」を作り出すことができるのであり、その手段のひとつが「安全確認型システム」なのです。

安全確認型の定義

安全確認型の定義は色々ありますが、一部の定義を除けば内容的には同じです。ここでは日本で初めて公式に定義された「JIS D 6802-1991「無人搬送車システム—安全通則」」の定義

「人と機械の共存システムにおいて、人の安全が確認されているときだけ、その機械装置やシステムの運転開始または継続を許可する構成を持つタイプ」を用いることにします。