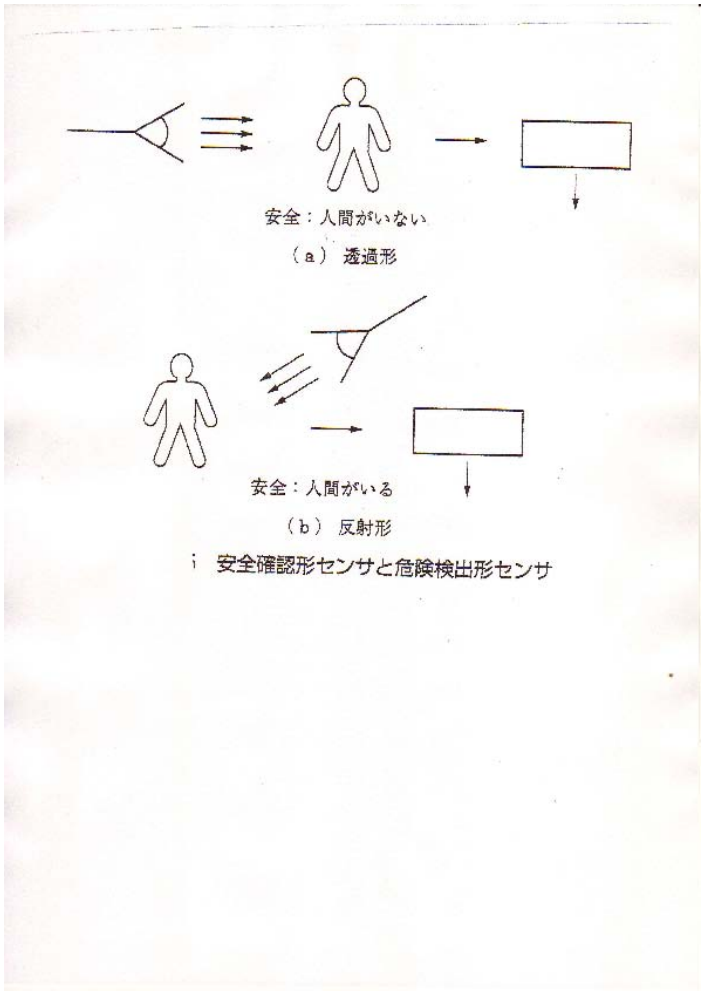
安全確認型に基づくフェールセーフな安全装置

明治大学理工学部　向殿政男

安全装置をフェールセーフに構成するための基本原理について紹介しましょう。安全装置は、一般にセンサー等の入力信号に従って状況を判断して、出力を変化させることにより、安全機能を果たしています。これには安全確認型と危険検出型の二つのタイプがあります。安全確認型は、安全であることを確認して、その安全確認信号に基づいて車を走らせたり、ロボットを稼動させたりする信号を出すものです。安全が確認できなくなったら車を走らせたり、ロボットを稼動させたりする信号が出なくなるタイプです。危険検出型は、危険であることをセンサー等で検出して、危険を回避する行動を取らせるタイプです。例えば、危険が検出されたら、車にブレーキを掛けたり、ロボットを止めたりする危険回避信号を出す形の安全装置です。危険が検出されない限り安全と解釈して、車の運転やロボットの稼動を続行させる形です。この二つの例を次の光センサーの例で説明しましょう。



安全確認型センサーと危険検出型センサー

センサーにより人間の存在を検出して、人間がいる時は危険としてロボット等を止める場合を想定します。図 5-1-5(a)は、安全確認型のセンサーの例です。光源から光を出し、受光器でこれを受けて、人間により光が遮断されない限り、人間が居ないので安全が確認されたとして、ロボット等を動かす信号が出されます。これは、透過型の光センサーとも言われます。図 5-1-5(b)は危険検出型のセンサーの例です。光源からの光を出し、人間が居る場合には、光が人間により反射されてそれを受光器で受けて、危険であることを知らせて、ロボット等を止める信号を出します。これは反射型の光センサーとも呼ばれます。危険検出型では、光源が故障しても、受光器が故障しても、出力の信号線が故障しても危険であることを知らせる信号は伝達されないので、人間が居るにもかかわらず、ロボット等は止まらないことになります。危険側故障です。安全確認型では、これらの故障はすべて安全を通達できなくなるので、人間が居なくても危険と見なしてロボット等は止まることになります。すなわち、安全側故障です。このように、壊れたら安全というフェールセーフな安全装置は、安全確認型でないと実現できません。安全装置のセンサーはついうっかり危険検出型で構成してしまう傾向がありますが、極力避けなければなりません。

更に、安全確認型を用いてフェールセーフに構成するためにはもう一つ注意しなければならないことがあります。安全であることを知らせる信号は、エネルギーの高い状態に対応させなければならないことです。これはハイボールの原理と呼ばれています(コラム参照)。安全確認型のセンサーの場合も、安全であることを示す状態は、エネルギーの高い状態が対応しています。危険検出型は逆で、危険であることをエネルギーの高い状態に対応させています。危険なことを知らせる信号にエネルギーの高い状態を対応させると、故障により伝わらないことがあるからである。エネルギーは故障により発散して消滅することはあり得ても、その逆はないという自然現象の非対称特性がここで利用されています。私たちの周りにある安全装置は、残念ながら以外に危険検出型が多いものです。

（向殿，北野他著、安全学入門～安全の確立から安心へ～、研成社、2009－8、pp.69-75より）