6Y-6　順序処理を用いたフェールソフトなフェールセーフ論理システム

坂井　正善　　向殿　政男
日本信号（株）　　明治大学

1．まえがき

ロボットと作業者の協調作業の様に人命に関わる分野では、システムの出力誤りに起因する最悪の事態の発生は絶対避けなければならないことが要請される。

フェールセーフ論理システムは予め定められた安全側にのみ出力誤りを生じる様に構成されたシステムで、上記要請を満足するシステムモデルの一つとして注目されている[1]。

ところで、システムの稼働率を考慮すると、ある程度の故障に対しては機能の一部を保存して動作する（フェールソフト）ようにシステムを構成することが望ましい。

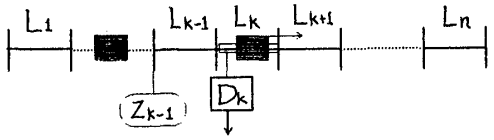
本報告では、システムを構成する要素の中で修復に時間を要すると考えられる検出装置の故障に対してフェールソフトな特性を持つフェールセーフ論理システムについて報告する。

本システムは、故障により失われた情報をフェールセーフな順序処理を用いて補正することによりフェールソフト性を実現することを特徴としている。これにより、一部の検出装置の故障に対してはシステムダウンを回避できる。

本文では、一方向のみに進む移動体の追突回避制御を例にとり、情報の変化に制約がある場合、上述の処理が可能であることを示す。次に、本構成法で用いる順序処理に要請される性質について簡単に述べる。

2．フェールソフトな閉塞システム

図．1に示す様に等間隔で区切られた走行路を区間Ｌ1からＬnに向かって一方向のみに移動体は進行するものとする。区間Ｌkへの進入許可信号をｚk（1/0で進入許可／禁止を表す）とし、移動体はこの進入許可信号が０である場合、一区間長以内で停止するものと仮定する。また、移動体の長さは区間の長さより短いものとする。



図．1　閉塞システム

以上の設定の基で、区間Ｌ1－Ｌn間に複数の移動体を走行させる場合の追突回避制御を考える。

Ｄkを区間Ｌkにおける移動体の有無を検出する装置とし、その検出信号は以下に示す様に与えられるものとする。

$$※k \triangleq xk \cdot dk \quad \cdots(1\text{-}1)$$
$$\neg ※k \triangleq \neg xk \cdot dk \quad \cdots(1\text{-}2)$$
（但し、　k=1,..,n）

ここに

$$xk \triangleq \begin{cases} 1 & \cdot\cdot \text{Lkに移動体が無し} \\ 0 & \cdot\cdot \text{Lkに移動体が有り} \end{cases}$$

$$dk \triangleq \begin{cases} 1 & \cdot\cdot \text{Dkが正常} \\ 0 & \cdot\cdot \text{Dkが故障} \end{cases}$$

※k（¬※k）は非対称誤り特性を持ち、検出装置Ｄkが正常でかつＬkに移動体が存在しない（する）時に限り１となる。

さて、

$$zk\text{-}1 \triangleq \begin{cases} ※1 \cdot ※2 & k=1 \\ ※k & k=2,..,n \end{cases} \quad \cdots(2)$$

で進入許可信号を生成した場合、Ｄkが故障するとｚk-1は０に固定されるので区間Ｌk-1に移動体は進入できなくなる（システムダウンを意味する）。

ところで、（ｘk-1,ｘk,ｘk+1）(k=2,..,n-1)

Fail-soft and Fail-safe Systems Utilizing Sequential Processings

Masayoshi Sakai　　Masao Mukaidono
Nippon Signal Co.,Ltd.　　Meiji Univ.

は図.2に示す様に一定の推移しかしない。

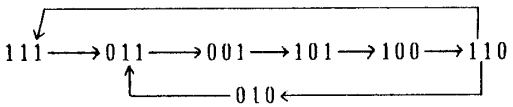
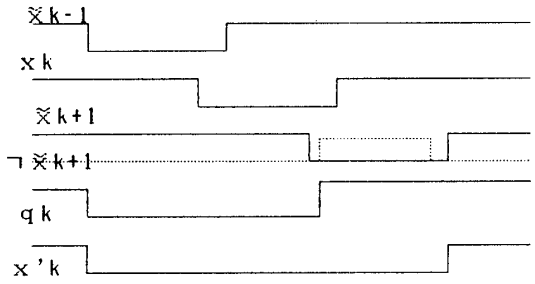


図.2　入力の推移

これを利用すると、Dkが故障して※kが0に固定された場合でも、移動体が区間Lkに存在しない(xk=1)ことを(※k-1,※k+1,¬※k+1)の推移を用いることにより以下に示す順序処理で確認することができる。　(タイムチャートは図.3参照)

$$\left.\begin{aligned} qk &\doteqdot ※k-1\cdot(qk+\neg ※k+1) \\ x'k &\doteqdot ※k+1\cdot qk \end{aligned}\right\} \cdots(3)$$

図.2より※k-1=※k+1=1であってもxk=1を結論できない。(3)式の処理は，図.2における(1,1,1)と(1,0,1)とを区別することに相当する。



図．3　順序処理のタイムチャート

図.3より、

$$x'k \leqq xk \quad \cdots(4)$$

なる単調性が成立していることがわかる。これは、(3)式の順序処理を用いて検出装置の情報を訂正しても誤って危険側に補正しないことを保証している。

$$zk-1=※k+x'k \quad (k=2,..,n-1)\cdots(5)$$

とすることにより、Dkが故障した場合でも区間Lk-1への進入は3区間(Lk-1,Lk,Lk+1)間隔が開けば許可されることになり、システムダウンが回避される。Dkが正常な場合は2区間(Lk-1とLk)間隔が開けば進入が許可されるので、この意味でフェールソフトな特性を持つと考えられる。

3．順序処理に課せられる単調性

図.4に本システムの処理ブロックを示す。mはフェールソフト性を実現するための順序回路、fは組合せ回路を表す。

Eを検出機構(複数の検出装置からなる)の故障の集合とし、e'≦eはe'の方がeより故障の程度が大きいことを意味するものとする。(例えば、2でe／e'がそれぞれDkのみ／DkとDk-1の故障を表すものとすると、e'≦e)また、便宜上λで故障のない状態を表しEの最大限とする。(i.e. ▽e∈E、e≦λ)

e∈Eなる故障により誤りを含んで検出機構より入力される信号をXeし、2で述べた検出機構の非対称誤り特性を仮定すると

▽e∈E、Xe≦Xλ

e'≦e　ならば　Xe'≦Xe

(例えば，2でXe≐(※k-1,※k,※k+1)e,Dkの故障をekとするとXek≦(1,0,1)であり，(1,1,1)となることはないから，Xek≦Xλ)

mにより誤り訂正された信号をX'とすると、本構成法では以下の制約を要することになる。

▽e∈E、X'≐m(Xe,Q)≦Xλ

(尚，Qはmの状態を表す)

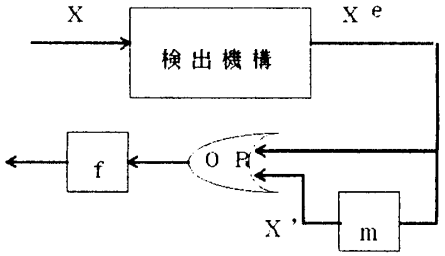


図.4　システムブロック

4．あとがき

本報告で述べたシステムはG－フェールセーフ論理システム[2]の一つの構成手法となっている。また、本構成法に必要な順序処理は非対称誤り特性を持つ(0に誤る)素子を用いて実際に回路実現可能である。

文献

[1]杉本,蓬原: 情報処理, 29-2(1988)

[2]向殿: 信学技報,PRL76-83,PRL77-43(1977)