

# TMR-FS 计算机控制系统的基本研究

周治邦

(上海铁道学院)

**关键词**——故障安全,安全侧,危险侧.

故障安全 (FS) 是计算机系统安全性设计中的重要基本概念之一. 本文将对严格同步的、三模冗余 FS 计算机控制系统(以下简称为 TMR-FS 系统)作一些基本研究.

## 一、FS 系统的形式定义

设  $S$  为任一系统.  $F = \{f_i | i = 1, 2, \dots, m\}$  是  $S$  的故障模式集合.  $\mathbf{z}_c(t)$  是  $S$  在无故障时的输出向量.  $\mathbf{z}(f_k, \mathbf{z}_c(t))$  是  $S$  在  $f_k (\forall f_k \in F)$  故障模式下的输出向量. 为简化符号,下文中将省去时间符号  $t$ .

记  $\tilde{Z}(f_k, \mathbf{z}_c) = \{\mathbf{z}(f_k, \mathbf{z}_c) | \mathbf{z}(f_k, \mathbf{z}_c) \neq \mathbf{z}_c\}$ .  $\tilde{Z}(f_k, \mathbf{z}_c)$  是对应于  $\mathbf{z}_c$  的,  $f_k$  故障模式可能引起的  $S$  的错误输出集合. 此外, 设  $\tilde{Z}(f_k, \mathbf{z}_c)$  划分成两个子集:  $\tilde{Z}_{sa}(f_k, \mathbf{z}_c)$  和  $\tilde{Z}_{da}(f_k, \mathbf{z}_c)$ , 它们满足

$$\begin{aligned} \tilde{Z}_{sa}(f_k, \mathbf{z}_c) \cup \tilde{Z}_{da}(f_k, \mathbf{z}_c) &= \tilde{Z}(f_k, \mathbf{z}_c), \\ \tilde{Z}_{sa}(f_k, \mathbf{z}_c) \cap \tilde{Z}_{da}(f_k, \mathbf{z}_c) &= \phi, \phi \text{ 是空集.} \end{aligned} \quad (1)$$

$\tilde{Z}_{sa}(f_k, \mathbf{z}_c)$  是  $S$  的(关于  $\mathbf{z}_c, f_k$  的,下同)安全侧错误输出集合,  $\tilde{Z}_{sa}(f_k, \mathbf{z}_c)$  中的每个输出向量对应于  $S$  的一个安全的或较为安全的操作.  $\tilde{Z}_{da}(f_k, \mathbf{z}_c)$  是  $S$  的危险侧错误输出集合,  $\tilde{Z}_{da}(f_k, \mathbf{z}_c)$  中的每个输出向量对应于  $S$  的一个危险性操作. 而  $\tilde{Z}_{sa}(f_k, \mathbf{z}_c) \cup \{\mathbf{z}_c\}$  是  $S$  的安全侧输出集合.

**定义 1.** 对于  $\forall f_k \in F$ , 若有  $\mathbf{z}(f_k, \mathbf{z}_c) \in \tilde{Z}_{sa}(f_k, \mathbf{z}_c) \cup \{\mathbf{z}_c\}$ , 称  $S$  是关于  $F$  的理想 FS 系统.

## 二、TMR-FS 基本构成原则

设  $V_{bi}$  是 TMR-FS 子系统  $i (i = 1, 2, 3)$  的总线表决器,  $V_p$  是 TMR-FS 的三取二输出表决器.  $C_b = \{c_{12}^b, c_{13}^b, c_{21}^b, c_{23}^b, c_{31}^b, c_{32}^b\}$  是 TMR-FS 的总线比较器;  $c_{ij}^b$  对  $i$  系的  $V_{bi}$  输出和  $j$  系总线上的数据作一致性比较, 当数据相同时,  $c_{ij}^b$  的输出  $z_{cij}^b = 1$ , 否则  $z_{cij}^b = 0$ .  $C_p = \{c_{12}^p, c_{23}^p, c_{31}^p\}$  是 TMR-FS 的输出比较器,  $c_{ij}^p$  比较  $i, j$  系通向  $V_p$  的输出接口上的数据, 相同时,  $c_{ij}^p$  的输出  $z_{cij}^p = 1$ , 否则  $z_{cij}^p = 0$ . 总线比较器和输出

比较器用于检测 TMR-FS 的错误数据流。此外,设  $F_{vp}$ 、 $F_c$  分别是  $V_p$ 、比较器的故障模式集合,  $F$ 、 $F_1$  分别是 TMR-FS 的故障模式集合和单模块故障模式集合。下面引入二个基本原则,据此可以构造一个实际的 TMR-FS 系统。

**原则 1.**  $\forall f_{vp} \in F_{vp}$ ; 若模块失效是相互独立的,且系统输出满足:  $z(f_{vp}, z_c) \in \tilde{Z}_{sa}(f_{vp}, z_c) \cup \{z_c\}$ , 则 TMR-FS 关于  $\forall f_k \in F_1 \cup F_{vp}$  是 FS 的。

令  $\omega = b, p$ . 设  $z_{cii}^a(f)$  是  $c_{ij}^a$  在  $f$  故障模式下的输出指示。

**原则 2.**  $\forall f_c \in F_c$ , 若  $f_c$  使  $c_{ij}^a$  失效时有  $z_{cii}^a(f_c) = 0$ , 则对于  $\forall f_k \in (F_1 \setminus F_{vp}) \cup F_c$ , 只要  $f_k$  导致错误发生且错误能够传播到总线或输出接口上, 那么必有: (1)  $\exists c_{ij}^b$ , 使  $z_{cii}^b(f_k) = 0$ ; 或者 (2)  $\exists c_{ij}^p$ , 使  $z_{cii}^p(f_k) = 0$ 。

原则 1 指出,设置 FS 输出表决器的 TMR-FS 系统具备 FS 特征; 而原则 2 指出,为正确检测错误数据流,  $c_{ij}^a$  必须是 FS 的,且 TMR-FS 应周期性地检测某些模块,使故障尽快传播到  $c_{ij}^a$ 。注意,  $V_p$  故障一般无法用  $c_{ij}^a$  检测,但  $V_p$  是 FS 的。通常将  $V_p$  的输出反馈到各个子系去判断它是否异常。

### 三、系统实现

图 1 是 TMR-FS 的系统结构(与子系  $A_1$  有关的电路), 它与文献 [1] 结构类似。

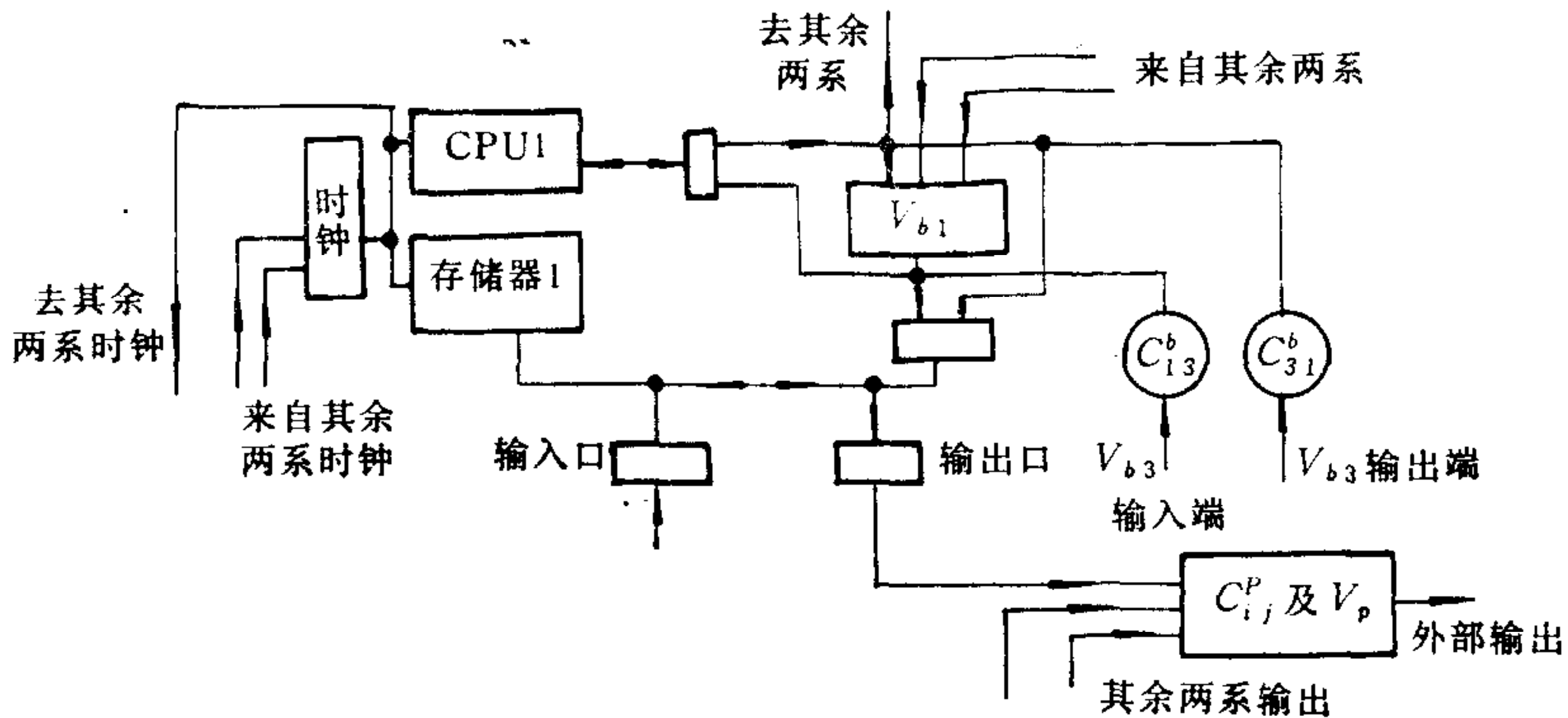


图 1

$V_{bi}(i = 1, 2, 3)$  可以由简单的与或门(或 PLA)构成。 $c_{ij}^b$  电路示于图 2, 其中  $c_x$  的逻辑方程为

$$\begin{aligned}
 P_1(n) &= P_0(n) \cdot \phi(n) + P_2(n-1) \cdot \phi(n) \cdot [R_i^b(n) \oplus R_j^b(n)], \quad n = 0, 1, 2, \dots, \\
 P_2(2l+1) &= P_2(2l+2) = P_1(2l), \quad l = 0, 1, 2, \dots, \quad \phi(2l) = 1; \quad \phi(2l+1) = 0, \\
 R_i^b(2l+1) &= R_i^b(2l+2); \quad R_j^b(2l+1) = R_j^b(2l+2), \quad (2)
 \end{aligned}$$

此外,  $P_0(n) = 0$ , 当  $n \geq 1$  时。初始条件为  $P_0(0) = P_2(-1) = P_2(0) = 1$ ,  $P_1(0_-) = 0$ ,  $R_i^b(0) = R_j^b(0) = 0$ 。 $P_1$  端振荡消失时,标志比较不一致发生。因  $\phi$  是单相时钟,故图 2 的实现较简单。

图 3 是  $V_p$  的逻辑电路,比较器  $c_{ij}^p$  已结合于  $V_p$  电路之中。图中  $y_{pj}(A_1)$ 、 $y_{pj}(A_2)$ 、

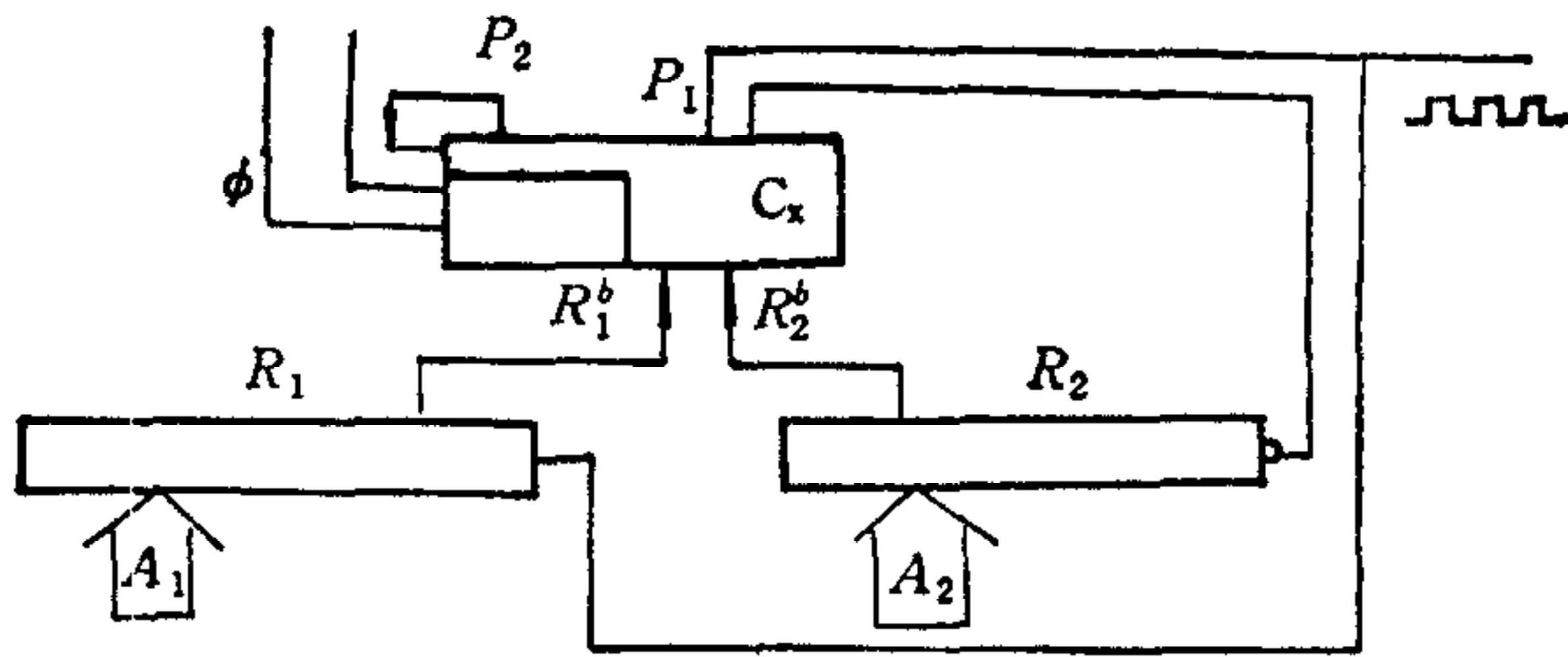


图 2

$y_{pj}(A_3)$  是三个子系  $A_1, A_2, A_3$  的输出,  $B_1, B_2, B_3$  是三个相同功能块. 图 3 模块的输出是振荡型的, 逻辑“1”表示有振荡波形.  $B_1$  的逻辑方程为

$$z_j^{B_1} = Q_1 \cdot [y_{pj}(A_1) \cdot y_{pj}(A_2)], \quad p_{x1} = z_j^{B_1}, \quad p_{x2} = \overline{y_{pj}(A_1) + y_{pj}(A_2)},$$

$$Q_1 = y_{pj}(A_1) \cdot y_{pj}(A_2) + p_{x2}. \quad (3)$$

当  $A_1, A_2$  输出不相同,  $Q_1 = 0$ , 指示比较不一致发生; 此时  $p_{x1} = p_{x2} = 0$ , 将  $T_x$  锁定在 0 侧. CV 的输出  $z_j$  提供给现场设备, 并反馈给各子系以检查外部输出是否为预定的正确性.

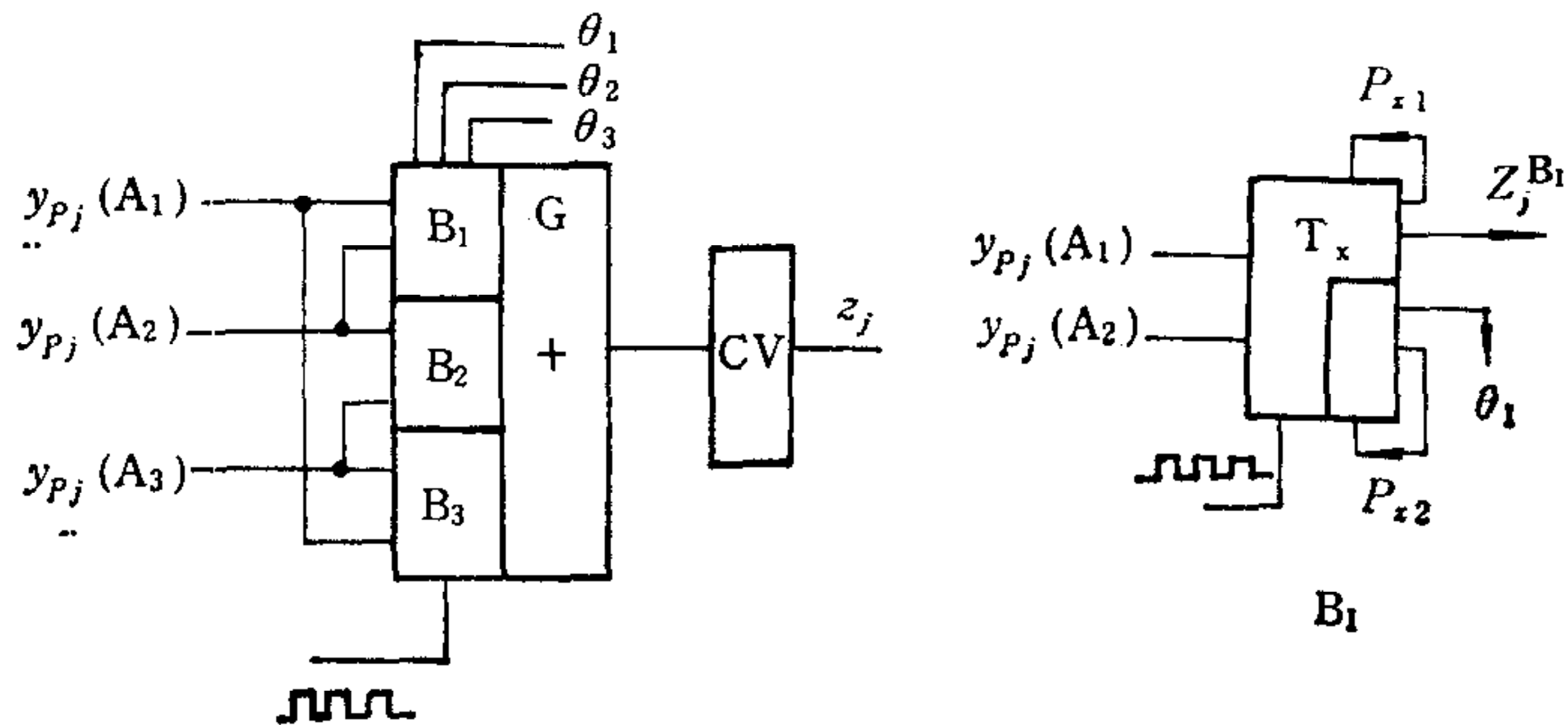


图 3

图 2, 3 能近似满足原则 1, 2, 它们只对电路的单故障和部分双故障是 FS 的.

感谢员春欣副教授的热情指导.

### 参 考 文 献

[1] Kwakubo, K., Nakamura, H., and Okumura, I., The Architecture of a Fail-safe and Fault-tolerant Computer for Railway Signalling Device, Proc. FTCS-10, 1980, 372-374.

## A BASIC STUDY OF A STRICTLY SYNCHRONOUS TMR-FS COMPUTER CONTROL SYSTEM

ZHOU ZHIBANG

(Shanghai Institute of Railway Technology)

**Key words**—Fail-safe; save side; dangerous side.