

综述与评论

# 故障安全逻辑系统的研究进程及 向自校验逻辑系统的演变

何文卿 邴 萌  
(北方交通大学) (上海铁道学院)

## 摘 要

本文简要地介绍了近十余年来关于故障安全逻辑系统和自校验逻辑系统的发展情况, 并指出这两者之间的区别和联系。文后列举了有关论文目录近一百条, 这些文献包括了这一时期内各阶段的主要研究成果。

近代电子技术和质量管理科学虽然能够使元器件的可靠性得到不断提高, 但由于计算机以及各类数字系统已经越来越深入到工业、交通、国防以至人们的日常生活领域, 所以一旦系统发生故障所带来的巨大经济损失和社会影响也越来越被人所重视。因此, 除了一般可靠性技术之外, 还需要在电路和系统设计中采用一种应付意外故障的手段, 即所谓故障安全 (Fail-safe, 以下简称 FS) 技术。

最早从理论上研究这一问题的有 J. Von Neumann、E. F. Moore 和 C. E. Shannon 等。在本世纪五十年代, 由于当时元器件可靠性不高, 他们分别提出用相同的低可靠性元件通过串并联或通过表决方式在元件发生故障时维持系统正常工作的方案<sup>[1,2]</sup>。这样的冗余技术, 目前已成为系统可靠性的专门课题和容错 (Fault-tolerant) 技术的一方面内容。由于不可能对系统内所有的部件(包括冗余转换和表决部件)都加以冗余, 因此单纯依靠冗余手段并不能完全解决问题。

1965年, 日本学者渡边昭治等首先提出 FS 逻辑系统的理论<sup>[3-7]</sup>。其中包括考虑冗余手段的故障安全问题<sup>[8,9]</sup>。

FS 的概念起源于铁路信号。世界上的第一条铁路, 即英国的斯多克顿—达林顿铁路上, 大风常常把夜间表示停车位置的蜡烛光吹灭而造成行车事故。后来采用利用重力自动转换成停车信号的信号机, 实现了 FS 的要求<sup>[10,11]</sup>。这种 FS 的概念近年来也被航空、原子能等领域所应用<sup>[12-14]</sup>, 成为一条以保障人身安全为目标的重要设计原则, 故障安全和以维持系统有效率为目标的可靠性意义不尽相同。渡边等人接受了传统的 FS 概念, 他们的研究具有以下特点:

- 1) 以现代半导体电子技术为基础; 2) 以离散结构、数理逻辑以及概率论等为理论工

具; 3) 以研究高速大系统的故障对策为目标. 因此, 和前面所述的具体设备的故障安全技术不同, 他们探索的是一般故障安全系统的构成规律. 为了区别起见, 把它称为 FS 逻辑理论. 渡边对 FS 所下的定义是: “一个逻辑系统在发生故障时, 能继续维持正常时的输出值或者转向某个预定的错误值 0 或 1, 则该系统为 FS 系统. 转向预定错误值 0 的称 0 型 FS 系统, 转向预定错误值 1 的称 1 型 FS 系统.” 他并根据与系统的输入错误是否有关这一点, 定义了强 (Strongly) FS 和弱 (Weakly) FS 的概念.

在此时期, 就这种来源于传统概念的二值 FS 逻辑理论发表论文的还有 H. Mine (三根久)、Y. Koga (古贺義亮)、川西健次和 S. Das 等<sup>[15-27]</sup>. 其中 H. Mine 和 Y. Koga 的文章证明严谨, 理论性强, 并且最早发表在 IEEE 的计算机汇刊上, 在国际上有较大的影响.

归纳上述论文, 二值 FS 逻辑和一般逻辑函数一样, 可看成是由输入空间上的点向输出空间的映射. 不同的是, 它必须满足下列条件:

设逻辑值 0 和 1 之间存在  $0 < 1$  的关系, 若系统出现任意故障  $f, f \in F$  ( $F$  为故障集), 在任意输入  $\mathbf{x}, \mathbf{x} \in X$  ( $\mathbf{x}$  为输入向量,  $X$  为输入集) 时, 其输出

$$Z(\mathbf{x}, f) \leq Z(\mathbf{x}), \text{ (对于 0 型 FS)}$$

或者

$$Z(\mathbf{x}, f) \geq Z(\mathbf{x}), \text{ (对于 1 型 FS)}$$

两者必居其一.

为了满足上述条件, 1) 要求制作出一种只出现 0 错误而不出现 1 错误, 或只出现 1 错误而不出现 0 错误的不对称出错元件 (Asymmetrically Fault Element, 以下简记为 AFE); 2) 要求系统的逻辑函数必须是单调 (Monotone) 函数或混合单调 (Unate) 函数; 3) 要求系统任一输出端的两个逻辑值确定地对应出错后两个不同的操作, 一个对应危险操作, 另一个对应安全或较为安全的操作. 这三点是实现二值 FS 系统的最基本的条件.

对于 AFE 进行研究并发表论文的有: 中道松郎、藤倉信之、土屋誠治、奥村幾正、川西健次等日本学者<sup>[28-41]</sup>. 其中有利用磁性材料、变参量元件、场效应管和以静态冗余、动态核对以及直流控制振荡等方式来实现的. 文献 [42] 和 [43] 则对 AFE 的性能作了综合分析. 我国就 AFE 发表文章的有王世亮、费锡康等<sup>[44,45]</sup>. 前者介绍的是 DC-AC-DC (振荡-恢复) 方式的厚膜集成 AFE 器件, 后者介绍调制和振荡方式的两种 AFE “与” 门. 这些器件均经过多年铁路现场使用的考验. 文献 [19] 和 [35] 所载的同类元件去年亦已用于微处理机故障安全冗余系统中<sup>[46]</sup>. 去年 Y. Koga 等人又发表了光电耦合元件方面的文章, 开辟了一条新的途径<sup>[47]</sup>.

日本的渡边、都倉、嵩、尾崎、T. Takaoka (高岡)、T. Ibaraki (茨木)、Y. Tohma (当麻) 和美国的 W. Potterson、G. Metzger、D. Sawin、L. L. Wang 和 Y. H. Chuang 等对 FS 时序电路开展了研究, 发表了不少文章<sup>[48-62]</sup>. 这些文章基本上分为采用 AFE 和采用一般元件实现 FS 两类.

利用二值 FS 逻辑实现铁路信号用计算机控制的, 有奥村幾正等人的文章<sup>[41,46,63]</sup>. 利用 FS 转接装置来提高混合冗余系统可靠性的有 R. C. Ogus 的文章<sup>[64]</sup>. 对二值 FS 系统利用概率进行定量评价的有中道松郎和郇萌等的文章<sup>[10,43,65]</sup>.

实现二值 FS 系统的第三个基本条件对某些实际系统是不存在的。此外,也不易满足函数单调性的要求。这就限制了二值 FS 系统的应用,因为在某些系统中,0 和 1 不一定意味着一方比另一方更安全。所以一些学者提出了一些新的 Fail-safe 的概念。

浦野義赖和向殿政男分别提出了两种三值的 FS 逻辑系统。前者称为  $\phi$  型<sup>[66]</sup>。后者称为 C 型<sup>[67]</sup>。两者都用额定的正、负电平对应 1 和 0 两个逻辑值,以地线电平为故障值。 $\phi$  型系统的故障值为  $\phi$ , C 型系统的故障值为  $1/2$ 。由于在这些系统中逻辑“0”和逻辑“1”的地位是完全均衡的,因此,二值 FS 系统中第二和第三两条要求在三值系统中不复存在。 $\phi$  型和 C 型三值系统的区别在于它们的运算规则不同。 $\phi$  型系统的三个值 1,  $\phi$ , 0 之间存在全顺序关系。因此有  $\phi \vee 1 = 1$  和  $\phi \cdot 0 = 0$  的运算。这使系统输出对于  $\forall f \in F$ ,  $\forall x \in X$  满足

$$Z(x, f) = Z(x)$$

或

$$Z(x, f) = \phi,$$

两者必居其一。

而 C 型系统 1,  $1/2$ , 0 三个值之间都是按特殊的定义来进行运算的。这些运算是  $1/2 \vee 1 = 1/2$ ;  $1/2 \vee 0 = 1/2$ ;  $1/2 \cdot 1 = 1/2$ ;  $1/2 \cdot 0 = 1/2$ 。因此,对于  $\forall f \in F$ ,  $\forall x \in X$  始终满足

$$Z(x, f) = 1/2.$$

作者把  $\phi$  和  $1/2$  看成是一个存在于正常逻辑值集合之外的安全输出,这对于不能从 0 或 1 出发找到安全与不安全含义的领域是有利的。取代二值 FS 系统第一个条件的三值逻辑器件的制作比二值器件更为复杂。除上述两种类型之外,中道松郎等还论述了其他几种三值逻辑<sup>[68]</sup>。三值 FS 逻辑的另一个问题在于它难以和一般逻辑电路兼容。于是, T. Takaoka (高岡)和 H. Mine (三根)提出了 N 型 FS 逻辑系统<sup>[69]</sup>。N 型 FS 系统也叫双轨系统,其逻辑值 1 和 0 均规定由一对二值电平信息偶组合而成。对于任意变量  $u = \langle u_1, u_2 \rangle$  定义

$$u = \begin{cases} 1, & \text{若 } \langle u_1, u_2 \rangle = \langle 1, 0 \rangle \\ 0, & \text{若 } \langle u_1, u_2 \rangle = \langle 0, 1 \rangle. \end{cases}$$

由于规定采用二值 1 型 AFE,把故障时出现的  $u = \langle 1, 1 \rangle$  (如使用 0 型 AFE 则为  $\langle 0, 0 \rangle$ ) 称为 N (Null 的意思),它的运算和  $\phi$  型三值逻辑系统相似,但它的电路本质上是二值的,很容易和一般逻辑元件兼容。特别是它的“非”(Not)运算只需将对应两根信息线交叉一下而不需使用单独的元件便可实现。需要指出的是 N 型 FS 系统中实际上已经在逻辑电路中引入了检错编码的思想,是二中取一的等比编码方式。同样,用  $\langle 0, 0 \rangle \rightarrow 0$ ;  $\langle 1, 1 \rangle \rightarrow 1$  的重复编码方式也可实现这类系统,但是奥村从故障概率上证明了  $\langle 1, 0 \rangle \rightarrow 1$ ;  $\langle 0, 1 \rangle \rightarrow 0$  的方式更为优越<sup>[41]</sup>。

上述各种有关 Fail-safe 的研究,当麻、奥村作了全面综述<sup>[70-72]</sup>。

需要指出,日本学者的这部分成果在当时是领先的。他们实际上已阐明了后来由美国学者提出的 Fault-secure 和 Self-testing 的概念。但是由于大部分文章没有得到在国外发表的机会,所以其成果并未为国外同行充分了解。日本学者原先认为不论是上述三值系统也好, N 型系统也好,都起源于传统的 Fail-safe 概念。由于这些研究和传统 Fail-safe

的研究在日本是连续进行的, 就沿用了 Fail-safe 的叫法. 但是 Safe 的含义如果不作特别的说明, 在有的技术领域会找不到相应的解释, 这就在其他国家引起了某些误解<sup>[73]</sup>.

美国在容错 (Fault-tolerant) 方面的研究开始得较早, 但是比较多的文章着重在冗余技术方面. 1968 年 W. C. Carter 对故障引起的逻辑错误, 提出用编码进行检测的电路<sup>[74-76]</sup>. 之后 D. A. Anderson 和 G. Metzger, R. W. Cook, J. F. Wakerly, S. M. Reddy, M. Diaz, J. M. Ashjase, J. E. Smith, A. Svoboda, M. A. Marouf, A. D. Friedman, B. Parhami, D. J. Lu 等发表了一系列这方面的文章<sup>[77-88]</sup>. 文献 [78], [80] 对上述文章中提到的自校验 (Self-checking) 下了较好的理论定义.

Anderson 提出, 判断自校验电路是否存在, 决定于是否能同时满足以下两个条件:

(1) Fault-secure 条件, 对于  $\forall \mathbf{x} \in I$  ( $I$  为输入空间上输入集  $X$  的子集) 和  $\forall f \in F_s$  ( $F_s$  为 Secure 故障集, 是故障集  $F$  的子集) 满足

$$Z(\mathbf{x}, f) = Z(\mathbf{x}) \in S$$

或

$$Z(\mathbf{x}, f) \notin S.$$

( $S$  是输出空间中符合编码规则的码字集合) 两者必居其一. 这里的 Fault-secure 可以译为失效保险, 也有人译为故障安全. 从上面叙述可以看出, 它和传统意义上的 Fail-safe 在概念上是不完全相同的.

(2) Self-testing 条件, 对于  $\forall f \in F_t$  ( $F_t$  为可测故障集, 是  $F$  的子集) 存在  $\exists \mathbf{x} \in X$  满足

$$Z(\mathbf{x}, f) \notin S.$$

Self-testing 可译为自测试.

J. F. Wakerly 把  $I$  集合中包含全部、一部分和一个也不包含  $X$  集合元素的三种情况定义为“完全自校验”、“部分自校验”和“单一自测试”三种类型.

可以看出 N 型双轨系统实质上是按“2 中取 1”方式编码的 Fault-secure 系统. 而 C 型三值系统则是  $F_s = F_t$  的完全自校验系统. 文献 [52] 中关于“用对称出错元件构成 FS”的提法也和自校验的定义是一致的. 自 1971 年第一次国际容错计算会议 (FTCS) 以来的各次会议, 自校验电路始终列为专门的征文选题, 而 Fail-safe 只在其中几次列为征文选题. 因此在这个领域中以自校验题目发表论文的越来越多, 如文献 [89], [90] 讨论的便是脱胎于 N 型和 C 型系统思想的自校验系统. 关于自校验和 Fail-safe 的联系, 文献 [91] 作了综述. 此外 S. S. Yan 还发表了软件自校验方面的文章<sup>[92]</sup>. K. F. Kapavoy 等评价了自校验的性能<sup>[93]</sup>.

上述论文, 大多是对自校验局部电路的讨论, 编码方式以“ $n$  中取  $k$ ”居多, 少数文章考虑了 Berger 码方式, 但是一个系统如何实现自校验的文章发表的不多.

我国, 杨樱华等在 FTCS-10 上发表了  $I^2L$  电路的完全自校验电路的论文<sup>[94]</sup>, 是国内较早的一篇.

实现自校验的一个重要条件是要制作一个可以不考虑失效的“硬核” (Hardcore), 这点在具体设备中要加以特殊考虑.

不论是 Fail-safe 还是 Self-checking 的研究, 其最终目标都是为了实现超高可靠性的计算机和其他数字系统. W. H. Pierce 在文献 [95] 中就提出容错计算机的设计问题. 当

麻、奥村也发表过这方面的论文<sup>[96,97]</sup>。K. Kawakubo 的文献 [46] 则介绍了已交付使用的一种 Fail-safe 冗余计算机系统。

十五年来关于数字系统中硬件故障对策的研究，从故障安全或自校验的理论来看已经有了较大的进展。今后期望不断解决电路的工作速度、同步和结构简化等难题，使它们更具有实用价值。当然实际电路将是各式各样的。因为它与所考虑系统的应用对象的具体情况有关，也与考虑容错后需要追加投资及经济收益的整体规划有关，还与各种电路的技术因素有关。

今后，如果在研制真正二值的 AFE 方面有所突破，相信对于容错技术的发展会有很大的推动。它不仅解决了 FS 系统的难题，也解决了自校验和冗余系统的硬核问题。

由于作者学识所限，所述很难全面。本文如果能给从事这方面工作的同行提供一点线索和方便的话，将感到由衷的高兴。

### 参 考 文 献

- [1] J. Von Neumann, Probabilistic Logics and the Synthesis of Reliable Organisms from Unreliable Components, *Annals of Mathematical Studies*, No. 34, Princeton Univ. Press, (1956) 43—98.
- [2] E. F. Moore, C. E. Shannon, Reliable Circuits Using Less Reliable Relays, *J. of Franklin Institute* **262**, (1956) 191—208.
- [3] 渡辺昭治、高橋泰司, Fail-safe 論理系の一構成法, 日本電子通信学会 (以下均簡記为 IECEJ) 大会文集, (1965).
- [4] 渡辺, FS 論理の基本性質と一般的構成法, IECEJ オートマトンと自動制御研究資料, (1966).
- [5] 渡辺, 浦野義頼, FS 論理系, IECEJ 会誌 (1967).
- [6] 平山、渡辺、浦野, Fail-safe 論理系の構成理論, *IECEJ Trans. (c)*, **52** (1969).
- [7] 山本、浦野、渡辺, 交番論理系のフェイルセーフ性, *IECEJ Trans. (c)*, **54** (1971).
- [8] 渡辺、高橋, Fail-safe 論理と誤り訂正機能のある二重系の一構成法, IECEJ 電算機研究資料, (1966).
- [9] 渡辺, 非対称誤り素子によるフェイルセーフ論理回路と二重化論理, IECEJ 会誌 (1967).
- [10] 日本信号保安協会, 鉄道信号発達史, 第八編: 信頼性・安全性, (1980).
- [11] 奥村幾正, 鉄道信号におけるフェイルセーフ, IECEJ 大会文集, (1974).
- [12] 島, 旅客輸送用航空機のフェイルセーフ, 同上.
- [13] 川口, 原子炉におけるフェイルセーフ, 同上.
- [14] 官尾, 高速エレベータのフェイルセーフ, 同上.
- [15] H. Mine, Y. Koga, Basis Properties and A Construction Method for Fail-safe Logical Systems, *IEEE Trans. EC-16*, (1967) 282—289.
- [16] 川西健次, Fail-safe, 日本電気学会誌, (1971).
- [17] 橋本、都倉、嵩, Fail-safe Logic and Duplicated Logic Through the Use of Asymmetrically faulty elements, IECEJ 会誌, (1967).
- [18] 宮田近昌, 一方向誤り素子によるフェイルセーフ論理回路の一構成法, *IECEJ Trans. (c)*, **52**, (1969).
- [19] 土屋誠治, フェイルセーフ論理方式の研究, 日本電気試験所報告, **695** (1969).
- [20] T. Takaoka, Algebraic Theory of Automata and Its Application to Fail-safe Systems, Ph. D. dissertation, Kyoto University, Japan, (1970).
- [21] N. Tokura, T. Kasami and A. Hashimoto, Fail-safe Logic Nets, *IEEE Trans.*, C-20 (1971).
- [22] Y. Koga, Studies on Logical System Analysis and Synthesis, Ph. D. dissertation, Kyoto University, Japan, (1971) 156—189.
- [23] 山本英雄, Fail-safe 論理回路を実現する素子条件について, *IECEJ Trans. (D)*, **55** (1972).
- [24] 三根久、茨木俊秀, FS システム, IECEJ 大会文集, (1972).
- [25] S. Das, Fault-tolerant Digital Systems Using Fail-safe Logic, D. Sc. dissertation, Dept. of Electrical Eng. Washington University, (1973).
- [26] 三根、古賀, Fail-safe システムの構成理論について, IECEJ 大会文集, (1974).
- [27] 三根、古賀, フェイルセーフシステムの安全性——理論的立場から, システムと制御, (1974).
- [28] 中道、渡辺, 入力相互の混觸を考慮したフェイルセーフ基本理論の提案, IECEJ 大会文集, (1967).

- [29] 中道, RC 結合マルチバイプレタを用いたフェイルセーフ論理回路, 同上.
- [30] 中道, トランスレスフェイルセーフ基本回路の一方式とその特性, IECEJ 大会文集, (1968).
- [31] 中道, フェイルセーフ論理回路の無接点繼電器への応用, 制御工学, (1969).
- [32] 中道, 特殊論理機能内部二重系 FSL の構成とその応用, IECEJ 大会文集, (1969).
- [33] 中道, 池田, 部品二重化非対称誤り素子による複合形セ FSL の構成とその特性, 同上.
- [34] 中道, FET による内部二重系準 FSL 基本回路の構成とその特性, IECEJ 大会文集, (1970).
- [35] 土屋, 三値 C 型フェイルセーフ論理回路, 日本計測自動制御学会論文集, (1970).
- [36] 中道, 藤倉, 池田, 交番駆動形 FSL の構成とその安全性解析, 日本計測自動制御学会資料 615, (1971).
- [37] 藤倉, 中道, 動的動作状態をもつ各種準 FSL の構成と問題点, IECEJ 大会文集, (1972).
- [38] 中道, 複合三値準 FS 論理系の危険側故障検出特性と機能制御による単純化, IECEJ 大会文集, (1973).
- [39] 渡辺, パラメトロによるセフェイルセーフ論理系, IECEJ 研究資料, (1965).
- [40] 川西, 磁性線を用いたフェイルセーフ論理素子, IECEJ 研究資料, NM43-23, (1969).
- [41] 奥村, 鉄道信号用連動装置のハードウェアに関するフェイルセーフ構成法, 日本電気学会論文集 (C), (1975).
- [42] 中道, 池田, 藤倉, フェイルセーフ論理素子の非対称誤り化構成則の考察, *IECEJ Trans. (D)*, 59 (1976).
- [43] 中道, 池田, 藤倉, フェイルセーフ論理素子の分類と評価, 同上.
- [44] 王世亮, 郇萌, 江涵, 馬樹祥, 故障安全逻辑厚膜元件及应用, 铁道学报, 2(1980), 58-66.
- [45] 費錫康, 两种安全型晶体管“与”门, 铁道信号论文集, 中国铁道出版社 (1980), 54-67.
- [46] K. Kawakubo, H. Nakamura and I. Okumura, The Architecture of a Fail-safe and Fault-tolerant computer for Railway Signalling Device, *Proc. FTCS-10*, (1980), 372-374.
- [47] Y. Koga, Y. Suzuki and K. Mizukami, Logic Elements for Fail-safe Circuit Design, 同上, 351-353.
- [48] 渡辺, 高橋, 榎本, FS 順序回路の一構成法, IECEJ 大会文集, (1966).
- [49] 都倉信樹, 嵩忠雄, 尾崎弘, FS 順序回路について, IECEJ オートマトンと自動制御研究資料, (1966).
- [50] Y. Tohma Y. Okayama and R. Sakai, Realization of Fail-safe Sequential Machines by Using a k-out-of-n code, *IEEE Trans. C-20* (1971).
- [51] 当麻喜弘, フリップフロップを用いたフェイルセーフ順序機械の構成法, *IECEJ Trans. (C)*, 54 (1971).
- [52] 当麻, 対称誤りによつてフェイルセーフ構成法, *IECEJ Trans. (D)*, 55 (1972).
- [53] T. Takaoka and T. Ibaraki, Fail-safe Realization of Sequential Machines, *Information and Control*, 22 (1973).
- [54] M. Diaz, T. C. Geffroy and M. Courvoisier, On-set Realization of Fail-safe Sequential Machines, *IEEE Trans., C-23* (1974).
- [55] W. W. Patterson and G. Metze, A Fail-safe Asynchronous Sequential Machine, 同上.
- [56] Y. Mukai and Y. Tohma, A Method for the Realization of Fail-safe Asynchronous Sequential Circuit, 同上.
- [57] Y. Tohma, Design Technique of FS Sequential Memory, 同上.
- [58] S. Das and H. Y. H. Chuang, United Approach to the Realization of Fail-safe Sequential Machines, *FTCS-4* (1974).
- [59] D. H. Sawin, Fail-safe Synchronous Sequential Machines Using Modified On-Set Realization, 同上.
- [60] L. L. Wang and H. Y. H. Chuang, On the Improvement of F-S Synchronous Machine Design Using On-Set Realization, *FTCS-5*, (1975).
- [61] H. Y. H. Chuang, FS Asynchronous Machines with Multiple Input Changes, 同上.
- [62] D. H. Sawin and G. K. Maki, FS Asynchronous Sequential Machines, *IEEE Trans., C-24*, (1975).
- [63] I. Okumura, Electronic Interlocking to be Tried in Japan, *Railway Gazette International*, (1980).
- [64] R. C. Ogus, Fault-tolerant of the Iterative Cell Array Switch for Hybrid Redundancy, *IEEE Trans., C-23* (1974).
- [65] 郇萌, 史定华, 二值故障安全系统的性能指标, 上海铁道学院学报, 1, (1980).
- [66] 浦野, 平山, 渡辺, φ型 Fail-safe 論理系, IECEJ オートマトン研究資料, A67-41, (1967).
- [67] 向殿政男, C 型フェイルセーフ論理の数学構造, *IECEJ Trans. (C)*, 54 (1969).
- [68] 中道, 伊藤, 梁, 故障検出容易なる種の三値論理とその応用, IECEJ 研究資料, (1977).
- [69] T. Takaoka and H. Mine, N-fail-safe Logic System, *IEEE Trans., C-20*, (1971).
- [70] 当麻, フェイルセーフ理論, (日本)電子科学, (1974).
- [71] 当麻, フェイルセーフシステムの理論, IECEJ 研究資料, R77-6, (1977).
- [72] 奥村, フェイルセーフの展望, IECEJ 会誌, (1979).
- [73] M. A. Breuer and Friedman, *Diagnosis & Reliable Design of Digital System*, Computer Science Press., (1976).
- [74] W. C. Carter and P. R. Schneider, Design of Dynamically Checked Computer, IFIP, (1968).

- [75] W. C. Carter, D. C. Sessep and A. Wadia, Error-free Decoding for Failure-tolerant-Mamories, *IEEE Trans.*, C-19 (1970).
- [76] W. C. Carter, A Simple Self-testing Decoder Checking Circuit, *IEEE Trans.*, C-20 (1971).
- [77] D. A. Anderson, Design of Self-checking, *IEEE Trans.*, C-20 (1971).
- [78] D.A. Anderson and G. Metze, Design of Tolerant Self-checking Check Circuit, *IEEE Trans.*, C-22 (1973).
- [79] R. W. Cook, W. H. Sisson, T. F. Storey and W. N. Toy, Design of A Self-checking Microprogram Control, *IEEE Trans.* C-22 (1973).
- [80] J. F. Wakerly, Partial Self-checking Circuit and Their Use in Perform Logical Operations, *IEEE Trans.*, C-23 (1974).
- [81] S. M. Reddy, A Note of Self-Checking checker, 同上.
- [82] M. Diaz, Design of Totally Self-checking and Fail-safe Sequential Machines, FTCS-4, (1974).
- [83] A. Svoboda, Self-checking Adder for Large Scale Integration, 3rd Symposium on Computer Arithmetic, (1975).
- [84] M. J. Ashjase and S. M. Reddy, On Totally Self-checking Checker for Seperable Codes, *IEEE Trans.*, C-26, (1977).
- [85] M. A. Marouf and A. D. Friedman, Efficient Design of Self-checking Checker for m-out-of-n Codes, FTCS-7 (1977).
- [86] M. A. Marouf and A. D. Friedman, Design of SC Checkers for Berger Codes, FTCS-8 (1978).
- [87] B. Darhomi, Totally SC Peripheral Circuit for Associative Devices, 同上.
- [88] D. J. Lu, Quantitative Comporsion of SC Circuit Design, 同上.
- [89] K. K. Hong and Y. Tohma, Signal Reliability Evolution of Self-checking Networks, FTCS-10 (1980).
- [90] 胡謀、K. C. Smith, 用 CMOS 三值门电路构成的一种自校驗二值逻辑系统, 计算机学报, 4(1981).
- [91] 奥村, セルフチェック回路の話題, IECEJ 大会文集, (1978).
- [92] S. S. Yan and R. C. Cheung, Design of Self-checking Software, PICRS, (1975).
- [93] M. F. Kapavoy and E. S. Sogomonyan, Compared Riliability Analysis of Redundancy Systems, FTCS-8 (1978).
- [94] Y. W. Yang, S. W. Liu and T. C. Chen, Threshold I<sup>2</sup>L Totally Self-checking Circuits, FTCS-10 (1980).
- [95] W. H. Pierce, Fault Tolerant Computer Design, Academic Press., (1965).
- [96] 当麻, Fault-tolerant Computing に関する2, 3の話題, 日本情報処理学会研究資料, (1975).
- [97] 奥村, フェイルセイフコンピュータ, IECEJ 会誌, (1978).

## PROGRESS IN THE RESEACH OF FAIL-SAFE LOGI CAL SYSTEM AND ITS EVOLUTION TO SELF-CHEC KING LOGICAL SYSTEM

HE WENQING

LI MENG

(Northern Jiaotong University) (Shanghai Institute of Railway Technology)

### ABSTRACT

In this paper, a brief survey is given to the development of fail-safe logical system and self-checking logical system in the past ten years and more, and their differences and relationships are pointed out. At the end of the paper, a bibliography of about hundred articles is given. Major results of the reseach in this field during that period were included in these articles.