文章编号：1005－8893（2002）04－0018－04

安全保护系统故障的可辨识性研究*

王凯全[1]，杨中利[2]
（1. 江苏石油化工学院 环境与安全工程系，江苏 常州 213016；2. 中金黄金股份有限公司，天津 300457）

摘要：安全保护系统在运行中可能出现“显性”和“隐性”2 种故障。为了实现安全保护系统对两类故障自辨识性，根据布尔差分理论，提出故障识别码的计算方法，并对上海高桥石化公司Ⅱ套催化裂化装置的安全保护系统进行了验证。

关键词：安全保护系统；故障；辨识
中图分类号：TP 213　　文献标识码：A

石化生产过程中存在着严重的潜在危险，安全保护系统（Safety Instrument System —— SIS）是检测潜在危险，预防生产事故的关键设备。然而，安全保护系统在运行中可能出现“隐性”（Inhibiting failure）和“显性”（Initiating failure）2 种故障。前者因“漏检”，将危险的生产状态误认为是安全状态，不能及时化解危险，可能造成生产事故；后者因“误检”，将安全的生产状态当成危险状态，强制中断生产，造成停产损失[1]。为了实现生产流程整体安全（Safety Integrity Level —— SIL），安全保护系统必须具备对 2 类故障的自检测能力，实现对自身故障的可辨识性。

目前，在石化流程中承担安全保护功能的核心部件是集散控制系统（Distributed Control System —— DCS）和紧急停车系统（Emergency Shutdown System —— ESD）中的组合逻辑单元。安全系统故障的可辨识性研究主要应解决的问题是，承载安全系统故障信息的状态参数能否正确地在组合逻辑单元输出端反映出来。具体地说，对于一个确定的组合逻辑单元，是否可以找到一些代表系统故障的测试码，当这些测试码输入组合逻辑单元后，通过检测其输出端信号的变化，确定其是否处于故障状态。如这样的测试码存在，则安全系统故障具有可辨识性[2]。

求组合逻辑单元测试码与输出码之间关系的方法是由阿凯思（Akers）等人首先提出的。本文运用这一方法，以布尔差分运算为基础，求出所需要的输入测试码，用来判断安全系统故障的可辨识性。

1　安全系统故障辨识原理

1.1　布尔差分及其性质[3]

假定有一组合逻辑单元，其初始输入的布尔变量记为 x_1，x_2，…，x_n，输出布尔函数记为 $f(x_1, x_2, \cdots, x_n)$，则有

$$\frac{\mathrm{d}f(X)}{\mathrm{d}x_i}=f(x_1, x_2, \cdots, x_{i-1}, x_i, x_{i+1}, \cdots, x_n)\oplus f(x_1, x_2, \cdots, x_{i-1}, \overline{x_i}, x_{i+1}, \cdots, x_n) \quad (1)$$

称为 $f(X)$ 对 x_i 的布尔差分。

布尔差分有以下 2 个重要性质。

性质 1　如果 $f(x_1, x_2, \cdots, x_{i-1}, 0, x_{i+1}, \cdots, x_n)=f(x_1, x_2, \cdots, x_{i-1}, 1, x_{i+1}, \cdots, x_n)$ 则有 $\frac{\mathrm{d}f(X)}{\mathrm{d}x_i}=0$ 即 x_i 处发生变化，对输出无影响，亦即 x_i 处的故障是不可测的。

性质 2　如果 $f(x_1, x_2, \cdots, x_{i-1}, 0, x_{i+1}, \cdots, x_n)\neq f(x_1, x_2, \cdots, x_{i-1}, 1, x_{i+1}, \cdots, x_n)$ 则有 $\frac{\mathrm{d}f(X)}{\mathrm{d}x_i}=1$

* 收稿日期：2002－07－22
作者简介：王凯全（1951－），男，上海人，副教授，博士，主要从事安全工程和信息管理方面的教学和科研工作。

即 x_i 处发生变化，对输出将有影响，亦即 x_i 处的故障是可测的。

1.2 系统故障测试码的计算

1.2.1 逻辑单元的故障模式

组合逻辑单元的故障有 2 种方式：

固定 1 故障（$s-a-1$）。对于布尔代数式

$$Z=x_1x_2x_3 \tag{2}$$

所表达的与门逻辑单元中，任何一个元素（如 x_1）取 1 时，Z 的值都不会因此而改变，即式（3）查不出固定数 1 的故障，因此称 x_1 是布尔代数式 Z 的固定 1 故障，简记为（$s-a-1$）故障。同样地，x_2、x_3 也是布尔代数式 Z 的固定 1 故障。

固定 0 故障（$s-a-0$）。对于布尔代数式

$$Z=x_1+x_2+x_3 \tag{3}$$

所表达的或门逻辑单元中，任何一个元素（如 x_1）取 0 时，Z 的值都不会因此而改变，即式（3）查不出固定数 0 的故障，因此称 x_1 是布尔代数式 Z 的固定 0 故障，简记为（$s-a-0$）故障。同样地，x_2、x_3 也是布尔代数式 Z 的固定 0 故障。

显然，安全保护系统的组合逻辑单元故障可测的条件是，这些单元不具有固定 1 和固定 0 故障。

1.2.2 单故障测试码的计算

阿凯思提出[3]，如果 $T(a_1, a_2, \cdots, a_n)$ 是被测通路 $X_i(x_1, x_2, \cdots, x_n)$ 上的固定 0 故障的测试码，则下式

$$X_i(x_1, x_2, \cdots, x_n)\times\left.\frac{\mathrm{d}f(X)}{\mathrm{d}x_i}\right|_{T(a_1, a_2, \cdots, a_n)}=1 \tag{4}$$

成立。式中 $a_i=0$ 或 1。

如果 $T(a_1, a_2, \cdots, a_n)$ 是被测通路 $X_i(x_1, x_2, \cdots, x_n)$ 上的固定 1 故障的测试码，则下式

$$\overline{X_i(x_1, x_2, \cdots, x_n)}\times\left.\frac{\mathrm{d}f(X)}{\mathrm{d}x_i}\right|_{T(a_1, a_2, \cdots, a_n)}=1 \tag{5}$$

成立。式中 $a_i=0$ 或 1。

应用（4）式、（5）式可以分别求出被测单元 $X_i(x_1, x_2, \cdots, x_n)$ 上同类型单故障（$s-a-0$）和（$s-a-1$）的测试码。例如，将由（4）式求得的测试码 $T(a_1, a_2, \cdots, a_n)$ 加到被测单元的标准输入端，如果被测单元的输出端 $z=1$，说明 $X_i(x_1, x_2, \cdots, x_n)$ 上无（$s-a-0$）故障，反之则有（$s-a-0$）故障。

2 安全保护系统故障的可测性实例

上海高桥石化公司 II 套催化裂化装置采用 *ESD* 系统进行安全监控[4]。图 1 为其核心部件的主要组合逻辑图。我们来考查其系统故障的可辨识性。

2.1 基本逻辑单元故障的可辨识性

在图 1 中，共有 3 种基本逻辑单元（图 2）。

对于图 2（a），因 $f(X)=x_1x_2+x_1x_3+x_2x_3$ 则

$$\frac{\mathrm{d}f(X)}{\mathrm{d}x_1}=(x_1x_2+x_1x_3+x_2x_3)\oplus(\overline{x_1}x_2+\overline{x_1}x_3+x_2x_3)=\overline{x_2}+\overline{x_3}+\overline{x_2x_3}$$

$$x_1\frac{\mathrm{d}f(X)}{\mathrm{d}x_1}=x_1(\overline{x_2}+\overline{x_3}+\overline{x_2x_3})$$

$$\overline{x_1}\frac{\mathrm{d}f(X)}{\mathrm{d}x_1}=\overline{x_1}(\overline{x_2}+\overline{x_3}+\overline{x_2x_3})$$

由对称性，有

$$x_2\frac{\mathrm{d}f(X)}{\mathrm{d}x_2}=x_2(\overline{x_1}+\overline{x_3}+\overline{x_1x_3})$$

$$\overline{x_2}\frac{\mathrm{d}f(X)}{\mathrm{d}x_2}=\overline{x_2}(\overline{x_1}+\overline{x_3}+\overline{x_1x_3})$$

$$x_3\frac{\mathrm{d}f(X)}{\mathrm{d}x_3}=x_3(\overline{x_1}+\overline{x_2}+\overline{x_1x_2})$$

$$\overline{x_3}\frac{\mathrm{d}f(X)}{\mathrm{d}x_3}=\overline{x_3}(\overline{x_1}+\overline{x_2}+\overline{x_1x_2})$$

类似地，对于图 2（b）、图 2（c），也可求出其单故障测试码的表达式。对于这些表达式，只要选择不同的 x_i 值（$x_i=1$ 或 0），总可以令其等于 1。所以，对于图 2（a）、图 2（b）、图 2（c）3 种组合逻辑方式，其故障是可以辨识的。表 1 为根据以上运算列出的各输入变量 $s-a-0$ 和 $s-a-1$ 故障识别码。

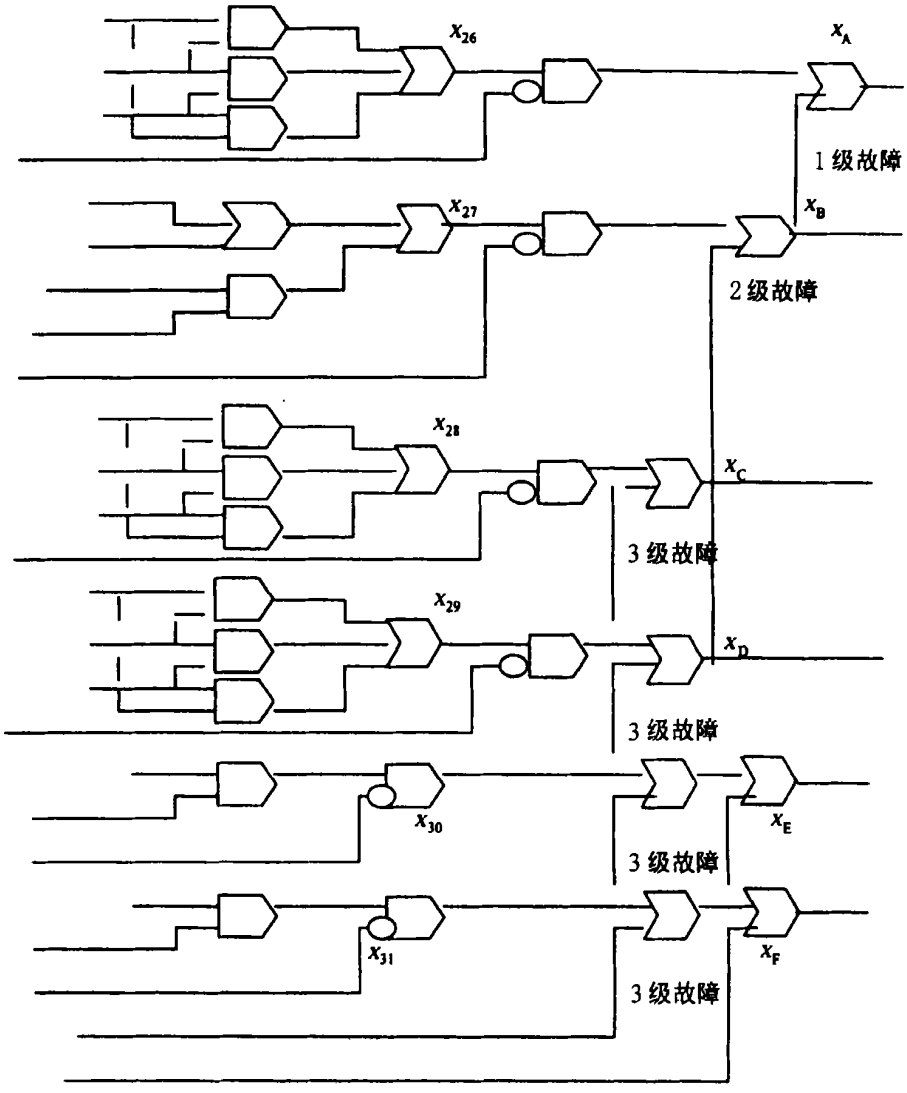

图 1 催化裂化核心控制部件的组合逻辑图

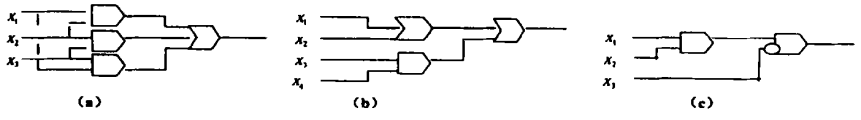

图 2 典型的组合逻辑单元

表 1 催化裂化典型组合逻辑单元输入变量故障识别码

故障模式		x_1	x_2	x_3	x_4
图 2(a)	$s-a-0$ 故障	{1, 0, 0}{1, 0, 1}{1, 1, 0}	{0, 1, 1}{0, 1, 0}{1, 1, 0}	{0, 0, 1}{0, 1, 1}{1, 0, 1}	
	$s-a-1$ 故障	{0, 0, 0}{0, 0, 1}{0, 1, 0}	{0, 0, 1}{0, 0, 0}{1, 0, 0}	{0, 0, 0}{0, 1, 0}{1, 0, 0}	
图 2(b)	$s-a-0$ 故障	{1, 0, 0, 0}{1, 0, 0, 1}{1, 0, 1, 0}	{1, 0, 0, 0}{1, 0, 0, 1}{1, 0, 1, 0}	{0, 0, 1, 1}	{0, 0, 1, 1}
	$s-a-1$ 故障	{0, 0, 0, 0}{0, 0, 0, 1}{0, 0, 1, 0}	{0, 0, 0, 0}{0, 0, 0, 1}{0, 0, 1, 0}	{0, 0, 0, 1}	{0, 0, 1, 0}
图 2(c)	$s-a-0$ 故障	{1, 1, 0}	{1, 1, 0}	{1, 1, 1}{1, 0, 1}{0, 1, 1}	
	$s-a-1$ 故障	{0, 1, 0}	{1, 0, 0}	{1, 1, 0}{1, 0, 0}{0, 1, 0}	

2.2 组合逻辑单元故障的可辨识性

以上述分析为基础，对催化裂化安全保护系统核心控制部件单元故障进行可辨识研究。

在图 1 中，有

$$x_A=(x_1x_2+x_1x_3+x_2x_3)\,\overline{x_4}+x_B=x_{26}\,\overline{x_4}+x_B$$

$$x_B=(x_5+x_6+x_7x_8)\,\overline{x_9}+x_C+x_D=x_{27}\,\overline{x_9}+x_C+x_D$$

$x_C=(x_{10}x_{11}+x_{10}x_{12}+x_{11}x_{12})\,\overline{x_{13}}+x_{24}=x_{28}\overline{x_{13}}+x_{24}$

$x_D=(x_{14}x_{15}+x_{14}x_{16}+x_{15}x_{16})\,\overline{x_{17}}+x_{24}=x_{29}\overline{x_{17}}+x_{24}$

$x_E=x_{18}x_{19}\overline{x_{20}}+x_{25}=x_{30}\overline{x_{20}}+x_{25}$

$x_F=x_{21}x_{22}\overline{x_{23}}+x_{24}+x_{25}=x_{31}\overline{x_{23}}+x_{24}+x_{25}$

式中：$x_{26}=x_1x_2+x_1x_3+x_2x_3$

$x_{27}=x_5+x_6+x_7x_8$

$x_{28}=x_{10}x_{11}+x_{10}x_{12}+x_{11}x_{12}$

$x_{29}=x_{14}x_{15}+x_{14}x_{16}+x_{15}x_{16}$

$x_{30}=x_{18}x_{19}$

$x_{31}=x_{21}x_{22}$

由于

$$\frac{\mathrm{d}f(X)}{\mathrm{d}x_{28}}=(x_{28}\overline{x_{13}}+x_{24})\oplus(\overline{x_{28}x_{13}}+x_{24})=\overline{x_{13}x_{24}}$$

所以

$$x_{28}\frac{\mathrm{d}f(X)}{\mathrm{d}x_{28}}=(x_{10}x_{11}+x_{10}x_{12}+x_{11}x_{12})\,\overline{x_{13}x_{14}}$$

$$\overline{x_{28}}\frac{\mathrm{d}f(X)}{\mathrm{d}x_{28}}=(\overline{x_{10}}+\overline{x_{11}})(\overline{x_{10}}+\overline{x_{12}})(\overline{x_{11}}+\overline{x_{12}})\,\overline{x_{13}x_{14}}$$

同样地，可以求出：

$$x_{29}\frac{\mathrm{d}f(X)}{\mathrm{d}x_{29}}=(x_{14}x_{15}+x_{14}x_{16}+x_{15}x_{16})\,\overline{x_{17}x_{24}}$$

$$\overline{x_{29}}\frac{\mathrm{d}f(X)}{\mathrm{d}x_{29}}=(\overline{x_{14}}+\overline{x_{15}})(\overline{x_{14}}+\overline{x_{16}})(\overline{x_{15}}+\overline{x_{16}})\,\overline{x_{17}x_{24}}$$

$$x_{30}\frac{\mathrm{d}f(X)}{\mathrm{d}x_{30}}=x_{30}\,\overline{x_{20}x_{25}}$$

$$\overline{x_{30}}\frac{\mathrm{d}f(X)}{\mathrm{d}x_{30}}=\overline{x_{30}x_{20}x_{25}}$$

$$x_{31}\frac{\mathrm{d}f(X)}{\mathrm{d}x_{31}}=x_{31}\,\overline{x_{23}x_{24}x_{25}}$$

$$\overline{x_{31}}\frac{\mathrm{d}f(X)}{\mathrm{d}x_{31}}=\overline{x_{31}x_{23}x_{24}x_{25}}$$

经过以上运算，同样获得催化裂化安全保护系统组合逻辑单元输入变量的单故障测试码。由于具体编码过于庞杂，本文不一一列出。

4 结 论

（1）提出了基于检测码方法的系统故障的辨识方法，并将其应用于实例之中。证明其系统故障是可辨识的，进而求出了其故障的检测码。

（2）研究表明：①根据布尔差分的性质，运用故障检测码可以发现某些安全保护系统自身的故障；②为了实现对安全保护系统故障的可辨识性，应合理设计其组合逻辑单元，使其具有检测码；③对于已判定为故障可辨识的系统，为了及时发现其自身故障，保证其能够正确查出生产过程中出现的各类事故隐患和偏差，应经常运用计算出的故障检测码对系统进行自检测。

参考文献：

[1] 王凯全. 石化流程的安全控制模型研究 [J]. 江苏石油化工学院学报，1999，11（4）：20－22.

[2] 唐永洪. 系统可靠性、故障诊断及容错 [M]. 重庆：重庆大学出版社，1990.

[3] 顾履平. 实用可靠性技术 [M]. 北京：机械工业出版社，1992.

[4] 王凯全. 催化裂化流程停车事故分析 [J]. 江苏石油化工学院学报，1998，10（1）：54－57.

Study on Failure Identification of Safety Instrument System

WANG Kai－quan[1]，YANG Zhong－li[2]

（1. Department of Environmental and Safety Engineering，Jiangsu Institute of Petrochemical Technology，Changzhou 213016，China；2. Huang Jin Inc. of China，Tianjin 300457）

Abstract：The Initiating failure and Inhibiting failure would occur in the period of SIS working. In order to identify the two failures by SIS itself，the paper proposed a mathematic method for finding the identification code based on the theory of Bayle derivation，and verified it on the FCC－Ⅱ Gaoqiao Petrochemical Company.

Key words：Safety Instrument System；failure；identification