Safety Voting System Based on D-S Evidence Theory

Yue Xi, Feng Liu, Hongli Yuan, Dongbo Pan*
Faculty of computer and information science, Southwest University, 2# Tiansheng Road, Beibei Dist., Chongqing, China, 400715
Corresponding author, e-mail: pandb@swu.edu.cn

Abstract

This thesis proposes a safety instrument system which is based on D-S evidence theory, including sensor, logic voting system and execution unit. While the logic voting system concludes the input circuit, processor, output circuit and the diagnosis module based on D-S evidence theory. According to the diagnosis module in multi-channel logic voting system and calculation based on D-S evidence theory, the interconnected feedback information can improve the reliability of the diagnosis. Therefore, the safety instrument system elaborated in this thesis can achieve system's self-diagnosis function under the premise of using less hardware equipment and at the mean time acquiring advantages of low cost, reliability and high security.

Keywords: *safety instrument system, safety function, D-S evidence theory, reliability*

1. Introduction

Safety Instrument System (SIS), also known as Safety Interlocking System, plays an important part in alarming and interlocking in industrial automatic control, whose function is implementing alarm system, adjusting or stopping the machines according to the testing results from the control systems [1, 2]. SIS shall execute its safety control function timely and correctly to prevent or reduce the occurrence of dangerous accidents, whereas accidents will happen.

At present, there are many methods for sa fety instrument system to achieve its safety function, among which probabilistic method is the most favorite way to measure security and risk assessment, such as Reliability Block Diagram (RBD) [3], Fault Tree Analysis (FTA) [4-6] and Markov Analysis (MA) [7-9] or Markov combined with other analysis [10], and so on. However, these methods still have some uncertain factors in assessing. The D-S evidence theory arose, which was first put forward by Dempster in 1967, further promoted and developed by Shafer in 1976. D-S evidence theory acquires unique advantages to solve the uncertainties mentioned above.

In view of the characteristics of D-S evidence theory and the present situation of safety instrument system, this thesis presents a safety instrument system based on D-S evidence theory, whose method is that under the multi-channel logic voting system structure and through proper calculation, whet her independent or interlocked channels, the output results will provide strong evidences for other channels. These evidences will form some certain or uncertain feedbacks so as to improve system's reliability and security, while D-S evidence theory exactly provides axiom system in processing the certainties and uncertainties. Therefore, the safety instrument system elaborated in this thesis can achieve system's self-diagnosis function under the premise of using less hardware equipment and at the mean time acquiring advantages of low cost, reliability and high security.

2. D-S Evidence Theory

2.1. Axiomatic System of Evidence

D-S evidence theory can be divided into probability distribution function, likelihood function and Despster evidence combination rule [11, 12]. Assume Frame of Discernment is θ, then function $m : 2^{\theta} \to [0,1]$ satisfies: $m(\phi) = 0$, $\sum_{A \cap \theta} m(A) = 1$ is called the basic probability

Received April 23, 2013; Revised June 22, 2013; Accepted July 24, 2013

distribution of frame of discernment θ. $\forall A \subset \theta$, $m(A)$ is the basic probability of A. The meaning of $m(A)$ is: if $A \subset \Omega$ and $A \neq \Omega$, thus $m(A)$ is the accurate trust degree of A; and if $A = \Omega$, thus $m(A)$ means it doesn't know how to allocate it.

As for $\forall A \subset \theta$, the defined function Bel: $m : 2^{\theta} \rightarrow [0,1]$ by $Bel(A) = \sum_{B \subset A} m(B)$ is the reliability function of θ. As for $\forall A \subset \theta$, pl is called the likelihood function of Bel in $pl(A) = 1 - Bel(\bar{A})$,

The relation of reliability function and likelihood function is that $Bel(A)$ and $pl(A)$ are respectively referred to the lower limit function and the upper limit function of $pl(A) \geq Bel(A)$.

2.2. Evidence Combination

Even the same evidences, due to different sources, the probability assignments will be different. Then D-S evidence theory puts forward to using orthogonal method to combine these functions.

Assume $m_1, m_2, \ldots, m_n$ are the basic probability assignment functions of 2^{Ω}, their orthogonal $m = m_1 \oplus m_2 \oplus \ldots \oplus m_n$ are:

$$\begin{cases} m(\varphi) = 0 \\ m(A) = k\square \sum_{\cap A_i = A} \prod_{1 \leq i \leq n} m_i(A_i), \quad A \neq \varphi \end{cases} \tag{1}$$

in which $k^{-1} = 1 - \sum_{\cap A_i = A} \prod_{1 \leq i \leq n} m_i(A_i)$.

2.3 Basic Algorithm

(1) It is known that: if we assume frame of discernment of some field is $\Omega = \{S_1, S_2, ..., S_n\}$, proposition A、B are the subsets of Ω, and the inference rule shall be:

$$if \quad E \quad then \quad H \quad , \quad CF$$

Among which E, H are the logic groupings of the proposition, CF is the certainty factor, and c_i means credibility. For any proposition A, the certainty factor CF of credibility A shall satisfy:

(a) $c_i \geq 0, 1 \leq i \leq n$

(b) $\sum_{1 \leq i \leq n} c_i \leq 1$

(2) Evidence Description: assume m is the defined basic probability assignment function of 2^{Ω}, then it shall meet the following conditions during calculation:

(a) $m(\{S_i\}) \geq 0, \quad S_i \in \Omega$

(b) $\sum_{1 \leq i \leq n} m(\{S_i\}) \geq 0 \leq 1$

(c) $m(\Omega) = 1 - \sum_{1 \leq i \leq n} m(\{S_i\})$

(d) $m(A) = 0, \quad A \subset \Omega, \quad and \quad |A| > 1 \quad or \quad |A| = 0$

among which $|A|$ means the factor numbers of proposition A.

(3) Inaccurate Inference Model

(a) Suppose A is one part proposition of regular condition, under the condition of evidence E , the matching degree of proposition A and evidence E is:

$$MD(A,E) = \begin{cases} 1, & if \quad E \supset A \\ 0, & Otherwise \end{cases} \tag{2}$$

(b) The definition of part proposition A in regular condition is:

$$CER = MD(A,E)\Box f(A)$$

3. Safety Instrument System Model based on D-S Evidence Theory

Safety instrument system, which is based on D-S evidence theory, includes sensor, logic voting system and execution unit. While the logic voting system concludes the input circuit, processor, output circuit and the diagnosis module based on D-S evidence theory. According to the diagnosis module in multi-channel logic voting system and calculation based on D-S evidence theory, the interconnected feedback information can improve the reliability of the diagnosis.

The following Figure 1 and Figure 2 are SIS traditional logic voting system structures. Take 1oo1 and 1oo2 for example. As it is shown in Figure 1, the 1oo1 system is the typical insecure system structure without redundancy and failure mode protection. While in Figure 2, 1oo2 system has two independent logic solvers. In order to disconnect the system reliably, the two output circuits adopt the method of serial connection. This system not only provides a low possibility of ineffectiveness, but also increases the possibility of fail safety circuit, which helps to improve the reliability of the system. The 1oo2D system in Figure 3 contains two independent electricpassages and diagnostic channels. If the output channel detects a potential dangerous failure, the system will automatically break the circuit in order to make sure the actuator in a safe state. The system's diagnostic function which uses "reference" method to diagnose system reflects in every channel. 1oo2D system not only can tolerate safety failure,but also danger failure. When it checks the first critical failure, the system will degrade to 1001D's function and by online main-taining, the system can return to 1oo2D structure. Figure 4 is the 1oo2 system structure with D-S diagnosis technology mentioned above.

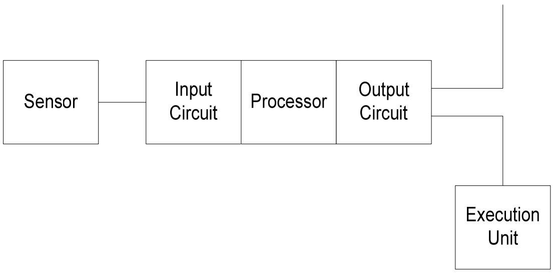

Figure 1. Typical 1oo1 System Structure in Logic Voting System

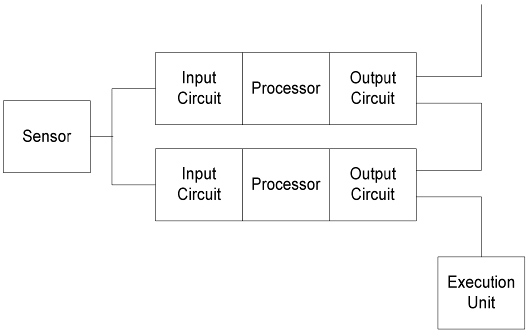

Figure 2. Typical 1oo2 System Structure in Logic Voting System

Further, logic voting system adopts 1oo2 structure. And the diagnosis module based on D-S evidence theory includes state-space identification module, function module and calculation module.

a) According to dual channel structure, state-space identification module determines the state and space, which will compose a frame of discernment θ. And these states will all together compose to a series of frame of discernments:
$\theta = \{\{\phi\},\{1\},\{0\},\{0,1\}\}$;

b) According to the reliability, function establishes modules and basic probability assignment function by frame of discernment $m:2^{\theta} \rightarrow [0,1]$, and last gets the basic probability assignment.

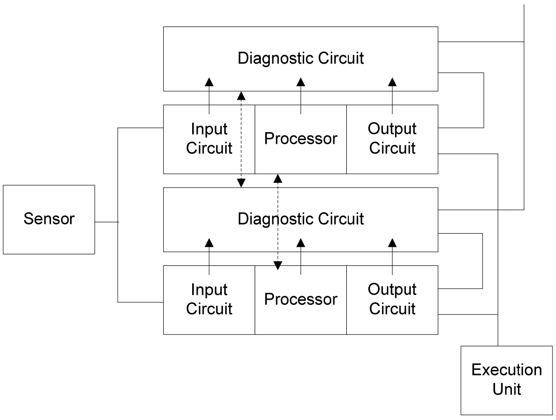

Figure 3. Typical 1oo2D System Structure in Logic Voting System

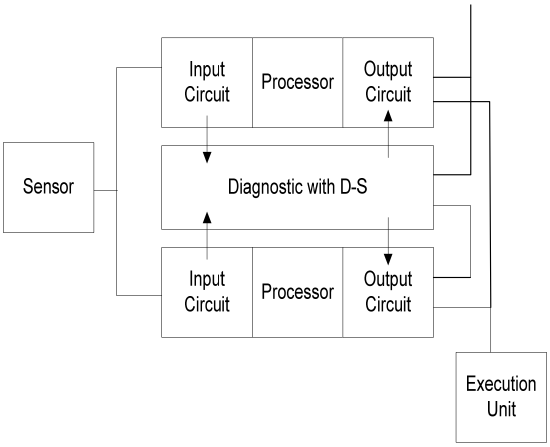

Figure 4. 1oo2 System Structure with D-S Diagnosis

For channel one:

$$m_x\{1\} = P(A_1 \mid A_2) \quad (3)$$

$$m_x\{0\} = P(\bar{A}_1 \mid \bar{A}_2) \quad (4)$$

$$m_x\{0,1\} = P(\bar{A}_1 A_2) + P(A_1 \bar{A}_2) \quad (5)$$

For channel two:

$$m_y\{1\} = P(A_2 \mid A_1) \quad (6)$$

$$m_y\{0\} = P(\bar{A}_2 \mid \bar{A}_1) \quad (7)$$

$$m_y\{0,1\} = P(\bar{A}_2 A_1) + P(A_2 \bar{A}_1) \quad (8)$$

c) According to probability assignment, calculation module calculates the orthogonal. It will first calculate $k^{-1} = \sum_{x \cap y \neq \varphi} m_x\{\bullet\} \times m_y\{\bullet\}$, and then $m\{\bullet\}$, thereby obtaining reliability measure.

The advantage of this system is that safety instrument system which is based on D-S evidence theory adopts the MooN logic voting system from D-S self-diagnosis technology. It has taken full use of redundant line of evidence function, which can produces strong feedbacks to the input signal correctly outputting and strengthening the output reliability. Compared to the MooN logic voting system of non-diagnosis technology, this can significantly improve the right output signal reliability and diagnostic coverage. Also, compared to the MooND system with diagnosis technology, D-S self-diagnosis technology can reduce the channel diagnosis circuit, almost acquire the performances of MooND system and at the mean time reduce the additional failure risk, improving system’s reliability and security.

4. Case Analysis

This part uses 1oo2 logic structure as a preferred case to elaborate the principle of safety voting system with D-S evidence algorithm. For each channel, there are two definite states {reliable}, {unreliable} and one indefinite state {unknown}. When {reliable} and {unreliable} are ex-pressed in channel one, channel two will give the same conclusion, which is described as {1}, {0}. While {unknown} is expressed in channel one, channel two will give opposite conclusion, which denote in {0,1}, and vice versa.

Assume channel one's reliability is 95%, and channel two's is 90%. Adopting 1oo2 structure, the correct output signal's reliability is 85.5%, while adopting 1oo2D, the correct output signal's reliability is above 99.5%. The failure possibility of using D-S diagnosis technology can be calculated as followed (suppose the two channels are independent):

For channel one:

$$m_x\{1\} = P(A_1 \mid A_2) = P(A_1) = 95\% \tag{9}$$

$$m_x\{0\} = P(\bar{A}_1 \mid \bar{A}_2) = 0.5\% \tag{10}$$

$$m_x\{0,1\} = P(\bar{A}_1\ A_2) + P(A_1\ \bar{A}_2) = 4.5\% \tag{11}$$

For channel two:

$$m_y\{1\} = P(A_2 \mid A_1) = P(A_2) = 90\% \tag{12}$$

$$m_y\{0\} = P(\bar{A}_2 \mid \bar{A}_1) = 0.5\% \tag{13}$$

$$m_y\{0,1\} = P(\bar{A}_2\ A_1) + P(A_2\ \bar{A}_1) = 9.5\% \tag{14}$$

so:

$$\begin{aligned} k^{-1} &= \sum_{x\cap y\neq\varphi} m_x\{\bullet\}\times m_y\{\bullet\} \\ &= m_x\{1\}\times m_y\{1\} + m_x\{1\}\times m_y\{0,1\} + m_x\{0\}\times m_y\{0\} + m_x\{0\}\times m_y\{0,1\} + \\ &\quad + m_x\{0,1\}\times m_y\{1\} + m_x\{0,1\}\times m_y\{0\} + m_x\{0,1\}\times m_y\{0,1\} \\ &= 0.99075 \end{aligned} \tag{15}$$

then:

$$\begin{aligned} m\{1\} &= k\sum_{x\cap y=\{1\}} m_x\{\bullet\}\times m_y\{\bullet\} \\ &= \frac{1}{0.99075}\times(m_x\{1\}\times m_y\{1\} + m_x\{0,1\}\times m_y\{1\} + m_x\{1\}\times m_y\{0,1\}) \\ &\approx 0.994953 \end{aligned} \tag{16}$$

$$\begin{aligned} m\{0\} &= k\sum_{x\cap y=\{0\}} m_x\{\bullet\}\times m_y\{\bullet\} \\ &= \frac{1}{0.99075}\times(m_x\{0\}\times m_y\{0\} + m_x\{0,1\}\times m_y\{0\} + m_x\{0\}\times m_y\{0,1\}) \\ &\approx 0.000732 \end{aligned} \tag{17}$$

$$\begin{aligned} m\{0,1\} &= k\sum_{x\cap y=\{0,1\}} m_x\{\bullet\}\times m_y\{\bullet\} \\ &= \frac{1}{0.99075}\times(m\{0,1\}\times m\{0,1\}) \\ &\approx 0.004315 \end{aligned} \tag{18}$$

Therefor, the reliable output signal of 1oo2 of D-S self-diagnosis technology is 99.4953%, which is significantly better than non-diagnosis technology of 1oo2 and is close to the 1oo2D structure with diagnosis circuit.

5. Conclusion

This thesis has proposed a safety voting system based on D-S evidence theory. When applied into case, the following conclusions can be drawn:

(1) To achieve the safety security function, the safety instrument system can provide axiom system in processing the feedbacks of channels' certainties and uncertainties. And according to the channels' interlocked feedbacks and based on the calculation of D-S evidence theory, it will improve the reliability of diagnosis.

(2) Safety voting system can achieve system's self-diagnosis function, improving SIS' reliability. Case analysis has shown that its output signal reliability is obviously better than non-diagnosis structure and is close to structure with diagnosis circuit.

(3) The cost of safety voting system reduces comparing with traditional systems. And it uses fewer hardware equipments to achieve the expected safety function. In the existing safety instrument system, logic voting system is either without self-diagnosis mechanism, or having complicated diagnostic circuit, which results in high cost. Therefore, the safety instrument system elaborated in this thesis can achieve system's self-diagnosis function under the premise of using less hardware equipment and at the mean time acquiring advantages of low cost, high availability and security.

Acknowledgements

We are grateful to our colleges and classmates Ya Li, Xiaoge Zhang and Xinyang Deng who introduced us to many of the topic discussed in this paper. Thanks are due to any anonymous referee for comments that helped increase the subjects covered in this paper. Partial finan-cial support from the National High Technology Research and Development Program of China (No. 2012AA041101), the Fundamental Research Founds for the Central Universities (No. XD-JK2013C029) are also gratefully acknowledged.

References

[1] International Electrotechnical Commission. IEC 61508. *Functional Safety of Electrical/Electronic/ Programmable Electronic Safety Related Systems*. Geneva: IEC Press; 2000.

[2] International Electrotechnical Commission. IEC 61511. *Functional Safety: Safety Instrumented Systems for the Process Industry Sector*. Geneva: IEC Press; 2003.

[3] Anatoly Lisnianski, Extended Block Diagram Method for a Multi-state System Reliability Assessment. *Reliability Engineering and System Safety*. 2007; 92: 1601-1607.

[4] Andrija Volkanovski, Marko Yepin and Borut Mavko. Application of the Fault tree Analysis for Assessment of Power System Reliability. *Reliability Engineering and System Safety*. 2009; 94: 1116-1127.

[5] GuoYan Chen, Xianggen Yin, Kai Zhang. Communication Modeling for Wide-Area Relay Protection Based on IEC 61850. *TELKOMNIKA*. 2012; 10(7): 1673-1684.

[6] GUO Haitao, YANG Xianhui. A Simple Reliability Blockdiagram Method for Safety Integrity Verification. *Reliability Engineering & System Safety*. 2007; 92(9): 1267-1273.

[7] GUO Haitao, YANG Xianhui. Quantitative Reliability Assessment for Safety Related Systems Using Markov Models. *Journal Tsinghua Univ (Sci &Tech)*. 2008; 48(1): 149-152,156.

[8] Hongsheng Su. Reliability and Security Analysis on Two-Cell Dynamic Redundant System. *TELKOMNIKA.* 2013; 11(5).

[9] B Knegtering, AC Brombacher. Application of Micro-Markov Models for Quantitative Safety Assessment to Determine Safety Integrity Levels as Defined by the IEC 61508 Standard for Functional Safety. *Reliability Engineering and System Safety*. 1999; 66: 171-175.

[10] Dongbo Pan, Hongli Yuan, Pengfei Xu, Feng Liu. Reliability of Safety Instrument System Based On Markov Model and D-S Evidence Theory. *Advanced Materials Research*. 2013.

[11] A Dempster. Upper and Lower Probabilities Induced by a Multivalued Mapping. *Annals of Mathematics and Statistics*. 1967; 38(2): 325-339.

[12] G Shafer. A Mathematical Theory of Evidence. Princeton: Princeton University Press. 1976.