2005 American Control Conference
June 8-10, 2005. Portland, OR, USA

A Cut/Tie Set Method for Reliability Evaluation of Control Systems

Hongbin Li[1] and Qing Zhao[1*]

Abstract— **This paper discusses the problem of reliability evaluation for control systems. The reliability evaluation in a system level provides an important criteria on the overall system operating performance and it can be used for guiding system reconfiguration upon the occurrence of a component failure. However, due to the dynamical and feedback relations among the elements in control systems, a valid reliability evaluation method is difficult to obtain by conventional approaches in reliability engineering. In this paper, an approach is introduced to evaluate the reliability by searching for the equivalent tie sets or cut sets based on the control system performance. When a fault is detected and identified on-line and/or the control objective is changed, the reliability can be easily re-evaluated by updating the cut sets or tie sets.**

I. Introduction

Reliability can be given as a probabilistic performance index on operation conditions and redundancy of components in a system, as well as tolerance of possible failures. For the Fault Tolerant Control (FTC) systems, reliability has always been a subjective concern. It is natural to make the ultimate goal of the FTC as to enhance the system reliability. However, there lacks quantitative measures for reliability in this context because the standard reliability assessment techniques are not geared toward the redundancy in the control systems [1]. Normal reliability analysis concerns with the series-parallel or network structures but few methods deal with the functional and dynamic relations involved in a control system. Hence, in the hybrid FTC systems, a linkage between the low-level control/diagnosis subsystems and the high-level decision/supervision module is missing [2].

In this work, we attempt to develop a method to describe the operating status of control systems in terms of reliability. Herein we are only interested in evaluating the reliability of the overall control system rather than individual component, and the reliability of each individual component is assumed to be known *a priori*. As a matter of fact, given a system, one can not always expect to improve the overall system reliability by using more reliable parts. On the other hand, we also know that even if some components fail, it is possible that the system reliability can be maintained at certain level. This fact indeed reflects the fundamental philosophy of the FTC systems. How to quantitatively assess the system level reliability in this context is still an open problem. There have been some investigations on this issue in the control community. In [3], the signal flow graph was adopted to perform the failure mode analysis but in this approach the control system was treated as the static system without considering the dynamics; fault tree analysis was used in [4], [5] but no control objective or dynamics were considered; functional-reliability modelling methods was employed in [6] but only a mean loss criterion instead of reliability was calculated; recent results were reported in [1], where an approximate Markov model was used to evaluate reliability and a criterion based on coverage was employed to bridge the control action and system reliability.

In this paper, we develop a procedure for reliability assessment of the control system by extending the tie/cut-set methods, which have been established for reliability analysis of networked systems. In the proposed method, the required functions of the system are related to control performance or control objectives. Furthermore, the procedure can easily cope with the change of the operating conditions of the system components and the number of performance requirements. When such change occurs, we only need to update the cut/tie set model and then re-calculate the reliability.

The remainder of this paper is organized as follows: In section II, the basic concepts about probability and reliability evaluation for network structures are briefly reviewed; the proposed methods are presented in section III followed by an example to illustrate the main procedures. The results in the example shows that simply changing loop gains in the control system can result in a change of system reliability. Section IV draws the conclusions.

II. Reliability evaluation of network structures

A commonly adopted definition of system reliability is given as follows [4].

Definition 1 (Reliability): The reliability, $R(t)$, of an item (a component or a system) is defined as the probability that, when operating under stated environmental conditions, it will perform its intended function adequately in the specified interval of time $[0, t]$.

Reliability block diagram is a graphical way to show the relationship between the functioning of the system and the functioning of its components. In practice, a system is often represented as a reliability block diagram in network structure in which the components are connected either in series, parallel, mesh or a combination of them. The cut/tie

[1] The authors are with Department of Electrical & Computer Engineering, University of Alberta, Edmonton, Alberta, Canada, T6G 2V4.

[*] The corresponding author. Tel: (780)492-5792; Fax: (780)492-1811; Email: qingzhao@ece.ualberta.ca.

0-7803-9098-9/05/$25.00 ©2005 AACC

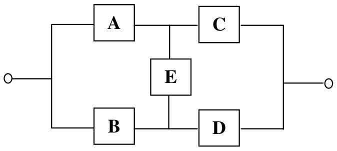

Fig. 1. Reliability block diagram in network structure.

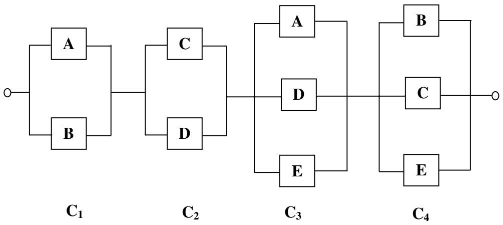

Fig. 2. Minimal cut sets diagram.

methods can be used to assess their reliabilities [7]. Note that in general feedback does not exist in a network.

A. Cut set method

Definition 2 (cut set): A cut set is a set of system components which, when fail, cause failure of the entire system.

Definition 3 (minimal cut set): A minimal cut set is a set of system components which, when fail, cause failure of the entire system; but when any one component in the set does not fail, the system will not fail as a whole.

From the definition, all components of each cut set must fail in order for the system to fail. Consequently, the components in one cut set are effectively connected in parallel. Furthermore, if there are more than one cut set, then the system fails if all the components in any one of the cut sets fails. Hence, all the cut sets are effectively connected in series. Therefore, given a system/network, one can obtain a simple parallel-series model based on the cut sets for the reliability analysis.

For example, the minimal cut sets of the system shown in Fig. 12.1 are $\{AB\}$, $\{CD\}$, $\{AED\}$ and $\{BEC\}$, which gives the reliability diagram of Fig. 2 for the network in Fig. 1. If the i-th cut is named as C_i and the probability of failure of all the components in C_i is represented by Pr(C_i), then the *reliability* is:

$$R_s = 1 - \text{Pr}(\overset{n}{\underset{i=1}{\cup}} C_i). \tag{1}$$

B. Tie set method

The tie set method is essentially the complement of the cut set method. A tie set is defined as a minimal path of the system and is therefore a set of system components connected in series. Consequently, a tie set fails if any one of the components in it fails and the probability can be evaluated using the principle of series systems. For the system to fail, all the tie sets must fail hence all tie sets are effectively connected in parallel. For example, the tie set diagram for the reliability block diagram of Fig. 1 is shown in Fig 3. Similarly, the concept of union of events applies when assessing the overall system reliability. For system shown in Fig. 3, the $reliability$ is:

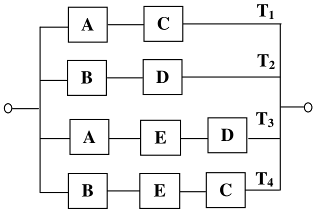

Fig. 3. Minimal tie sets diagram.

$$R_s = \text{Pr}(T_1 \cup T_2 \cup T_3 \cup T_4), \tag{2}$$

where T_i, $i = 1, 2, 3, 4$, is the i-th tie set. The above expression can be decomposed into Pr(T_i) which represents the probability that all the components in T_i work. Please note that the definitions of Pr(C_i) and Pr(T_i) are complementary.

The minimal cut/tie sets can be generated by standard algorithms, such as multiplication of the connection matrices, so the reliability evaluation methods based on minimal cut/tie set can be easily implemented on computers [7].

III. Reliability evaluation of control systems

In this part, we introduce a method to evaluate the reliability of a control system based on the failure analysis and the minimal cut/tie sets concepts. A control system is quite different from a network structure in two respects. Firstly, it involves feedbacks and dynamic relationships among all components; secondly, the concepts of "intended functions" (as mentioned in Definition 1) are different. In the network structure, as long as there exists a path from the starting node to the end node (represented by small circles in Fig 2.1), the network is deemed to be functional. But the control system should satisfy certain control objectives that can be described in various forms, such as system norms, system transient responses, and stability criteria, etc. Therefore, it is necessary to perform failure analysis first by taking account these dynamical relationships and control objectives.

A. A typical structure of control systems

Control systems are usually composed of four categories of components: controller, actuator, plant and sensor, which may have various configurations based on the particular application and control strategies. For failure and reliability analysis, it is difficult to develop a method to deal with all kinds of systems. Herein a standard control system configuration as shown in Fig. 4 is adopted, and the subsequent analysis can be conducted on this configuration.

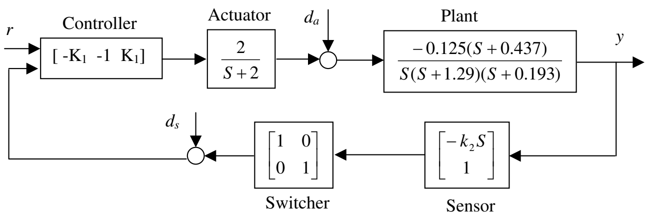

Fig. 4. Standard structure of control systems

- G_c, P, G_a and G_s stand for the controller, plant, actuators and sensors.
- r is the reference input signal; y, the output signal, is measured by the sensor.
- Matrices M, N and the signals d_a, d_s are used to model the failure modes of the actuators and sensors, which will be explained in the next section.
- The system in general is of multi-input and multi-output, hence the signal involved in this structure are vector signals and the transfer functions are in the form of transfer matrices.

B. Failure mode modeling

Physical systems and components are liable to fail. Roughly speaking, failure can be considered as the loss of designed functionality or the unacceptable deviation of the associated parameters in the systems or components. It is impractical to describe all kinds of failures in a unified expression. Considering that the actuators and sensors are the most vulnerable parts in control systems, we focus on modeling the failures of these components, which normally have the following four categories of failure modes:

- Stuck: the output is fixed at some constant values.
- Bias: the output contains a deviation from the expected value.
- Saturation: the output stays at the maximum and minimum values, due to the physical limitations.
- Loss of effectiveness: the gain between the output and input is reduced.

By introducing the switching matrix and the bias signal, we can easily model the first three failure modes. The switching matrix, M or N, is a diagonal and binary matrix connected in series with the component to represent whether there is signal flow through it or not. The bias is an external signal that introduces the deviation of the measurement signal. For instance, if there are 3 sensors, the failure scenario that the first one is stuck at 0.8 and the third one is saturated at 1 can be described by: switching matrix $N = \text{diag}(0,\ 1,\ 0)$ and bias $d_a = [0.8, 0, 1]^T$, where 'diag' represents a diagonal matrix.

Here, a single failure event occurred in a specific component is named as a basic failure. For a particular component, only one basic failure can occur at one time. All failure scenarios are simply the combinations of these basic failures. Suppose there are m kinds of basic failures denoted as f_1, f_2, $\cdots$, and f_m, each of which can be represented by assigning certain values to M, N, d_a and d_s. For the above example, the sensor failure scenario can be described by the following set:

$$\begin{aligned} F &= \{f_1 \text{ and } f_2\} = \{N(1,1) = 0,\ \ d_s(1) = 0.8 \\ &\quad \text{and } \ N(3,3) = 0,\ \ d_s(3) = 1\}. \end{aligned} \tag{3}$$

To be consistent with probability notation, we will use $f_i \cap f_j$ to represent the scenario when the basic failures f_i and f_j occur simultaneously, while $\bar{f}_i \cap \bar{f}_j$ stands for the event that neither f_i nor f_j occurs.

C. Cut sets and tie sets in control systems

The basic ides is to find the minimal cut/tie sets for a control system and thereby convert a dynamical system structure into the serial-parallel reliability block diagram as we have done on the network structure system. When a particular failure is detected, the new tie/cut sets are reconstructed by revising the original results and reliability updated. Thus, the cut/tie sets are essential to perform the reliability evaluation in control systems. Before evaluate reliability, the following assumptions are presumed.

1) The control objectives or the intended function to decide whether the control system succeed or not.
2) The dynamical relationships of all components or the mathematical model of the system.
3) The failure scenarios, including the failure modes for each components and the associated probability of occurrence.

Usually there are multiple requirements on control systems and the control objectives are described by a set:

$$O = \{O_1, \cdots, O_{n_o}\}. \tag{4}$$

where each element, O_i, is a statement of the system characteristics, such as stability, specifications on transient step response or system norm. For example,

$$O_1 = \{t_{\text{rise}} < 2\}, O_2 = \{\forall P_i, \Re\{P_i\} < -1\}.$$

t_{rise} represents the rising time, P_i the closed-loop pole and $\Re\{P_i\}$ its real part. When each element of the objective set is satisfied, the system is said to succeed under current failure mode; otherwise, system is considered to fail. Using this representation, the cut set and tie set are redefined for the control systems.

Definition 4 ((basic) minimal cut set): A (basic) minimal cut set for control system reliability analysis is a set of basic failures $C = \{f_1^c, \cdots, f_m^c\}$, which satisfies that: the intersection of all events in C causes violation of $O(O_i)$, while any subset of C does not cause the violation.

Definition 5 ((basic) minimal tie set): A (basic) minimal tie set for a control system is a set of basic failures $T = \{f_1^t, \cdots, f_m^t\}$, which satisfies that: any element in T

causes violation of the objective $O(O_i)$, while the objective $O(O_i)$ is satisfied if none of the events in T occurs.

Here we define basic cut/tie set according to the particular objective element O_i and the cut/tie sets according to objective set O. It follows the same rules to set up the serial-parallel reliability block diagram based on the cut sets or tie sets. Note that only minimal cut/tie sets are defined for control systems and the word, 'minimal', is sometimes omitted for brevity in the following sections.

D. Reliability calculation

Assume that all the minimal cut sets for a control systems are identified as:

$$\begin{aligned} C &= \{C_1, \cdots, C_n\} \\ &= \{\{f_1^{c_1}, \cdots, f_{m_1}^{c_1}\}, \cdots, \{f_1^{c_n}, \cdots, f_{m_n}^{c_n}\}\}, \end{aligned}$$

where $\{f_1^{c_i}, \cdots, f_{m_i}^{c_i}\}$ represents m_i basic failures in the i-th cut set C_i. Then, the reliability of the control system is:

$$\begin{aligned} R &= 1 - \Pr\{C_1 \cup \cdots \cup C_n\} \\ &= 1 - \Pr\{(f_1^{c_1} \cap \cdots \cap f_{m_1}^{c_1}) \cup \cdots \cup (f_1^{c_n} \cap \cdots \cap f_{m_n}^{c_n})\}. \quad (5) \end{aligned}$$

If all the minimal tie sets for a control systems have been identified as:

$$\begin{aligned} T &= \{T_1, \cdots, T_n\} \\ &= \{\{f_1^{t_1}, \cdots, f_{m_1}^{t_1}\}, \cdots, \{f_1^{t_n}, \cdots, f_{m_n}^{t_n}\}\}, \end{aligned}$$

then the reliability of the control systems is:

$$\begin{aligned} R &= \Pr\{T_1 \cup \cdots \cup T_n\} \\ &= \Pr\{(\bar{f}_1^{t_1} \cap \cdots \cap \bar{f}_{m_1}^{t_2}) \cup \cdots \cup (\bar{f}_1^{t_n} \cap \cdots \cap \bar{f}_{m_n}^{t_n})\}. \quad (6) \end{aligned}$$

where $\bar{f}_1^{t_1}$ represents that $f_1^{t_1}$ does not occur.

For the active FTC systems, the component failure can be diagnosed by a Fault Detection & Isolation (FDI) scheme on-line. Based on the FDI results, the reliability value can be updated by modifying cut/tie sets. For instance, if f_k is detected by FDI and we do not consider the false alarm, the new tie set or cut set is derived according to the rules below:

$$\begin{aligned} T_{\text{new}} &= \{T_i | T_i \in T, \quad f_k \notin T_i\}, \quad (7) \\ C_{\text{new}} &= \{C_i' | C_i' = C_i - \{f_k\}, C_i \in C, f_k \in C_i; \\ &\quad \text{or } C_i' = C_i, C_i \in C, f_k \notin C_i\}. \quad (8) \end{aligned}$$

The updated reliability can be computed by these new sets. If consider the false alarm of the FDI, for instance, if f_k is detected by FDI with probability $\hat{P}_k$ and the original probability is P_k, then the new probability is replaced by $\hat{P}_k$, or $P_k' = \hat{P}_k$, while the cut sets and tie sets remain unchanged. To illustrate the above method, let us look at an example.

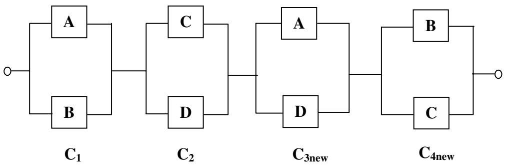

Fig. 5. Updated minimal cut sets diagram.

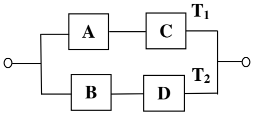

Fig. 6. Updated minimal tie sets diagram.

Assume for a particular control system the basic failure set is $F = \{A, \ B, \ C, \ D, \ E\}$, and the cut sets and tie sets are identified as:

$$\begin{aligned} \mathbf{C} &= \{C_1, \ C_2, \ C_3, \ C_4\} \\ &= \{\{A, \ B\}, \{C, \ D\}, \ \{A, \ D, \ E\}, \ \{B, \ C, \ E\}\}, \\ \mathbf{T} &= \{T_1, \ T_2, \ T_3, \ T4\} \\ &= \{\{A, \ C\}, \ \{B, \ D\}, \ \{A, \ E, \ D\}, \{B, \ E, \ C\}\}. \end{aligned}$$

The corresponding cut set diagram and tie set diagram are given in Fig. 2 and Fig. 3. According to the assumptions, the probabilities of the basic failures are known. Then the reliability of the control system can be computed as:

$$\begin{aligned} R &= 1 - \Pr\{F_{C_1} \cup F_{C_2} \cup F_{C_3} \cup F_{C_4}\} \\ &= 1 - \Pr\{(A \cap B) \cup (C \cap D) \cup (A \cap D \cap E) \cup (B \cap C \cap E)\}, \\ R &= \Pr\{F_{T_1} \cup F_{T_2} \cup F_{T_3} \cup F_{T_4}\} \\ &= \Pr\{(\bar{A} \cap \bar{C}) \cup (\bar{B} \cap \bar{D}) \cup (\bar{A} \cap \bar{E} \cap \bar{D}) \cup (\bar{B} \cap \bar{E} \cap \bar{C})\}. \end{aligned}$$

If the FDI indicates that failure E occurs, the updated cut sets and tie sets are:

$$\begin{aligned} C_{\text{new}} &= \{C_1, C_2, C_{3\text{new}}, C_{4\text{new}}\} \\ &= \{\{A, B\}, \{C, D\}, \{A, D\}, \{B, C\}\}, \\ T_{\text{new}} &= \{T_1, T_2\} = \{\{A, C\}, \{B, D\}\}. \end{aligned}$$

The corresponding updated diagrams are given in Fig. 5 and 6. Then the new reliability can be re-evaluated easily. On the other hand, if failure E is detected with a probability $\hat{P}_E$, then the probability of the occurrence of E is replaced by $\hat{P}_E$. The reliability can be re-assessed based on the updated probability and the same cut sets and tie sets.

E. Cascade cut set and tie set

In FTC systems, if some components suffer from failures, the requirements are usually relaxed by giving up certain performance. The system performance will be degraded but 'gracefully'. In this case, it is done by removing some elements in the objective set $O = \{O_1, \ \cdots, \ O_{n_o}\}$, so a new objective set is obtained, O'. Instead of repeating the whole reliability evaluation procedure when the objective set is changed, one simpler method is to search the cut/tie sets for each single objective O_i in O, $i = 1 \sim n_o$, and then derive the cut/tie sets for the entire set O. We name this method as cascade cut/tie set, which can reduce the computation during the re-evaluation when the objective set changes.

Suppose the basic cut/tie sets for each objective O_i, $i = 1 \sim n_o$, are given below as

$$C^i = \{C_1^i, \quad \cdots \quad C_{n_i}^i\}, \quad T^i = \{T_1^i, \quad \cdots \quad T_{m_i}^i\}.$$

Define the following two set operations.

- If $A = \{A_1, \cdots, A_n\}$, then compact$(A) = \{A_i | A_i \in A, \forall A_j \in A, A_j \nsubseteq A_i, j \neq i, i, j = 1 \sim n\}$.
- If $A = \{A_1, \cdots, A_n\}$, $B = \{B_1, \cdots, B_m\}$, then $A \times B = \{C_k | \exists\ i, j, i = 1 \sim n, j = 1 \sim m, C_k = A_i \cup B_j\}$.

Then, derive the cut/tie sets for O as follows:

$$\mathbf{C} \quad = \quad \text{compact}\{\bigcup_{i=1}^{n_o} C^i\}, \tag{9}$$

$$\mathbf{T} \quad = \quad \text{compact}\{T^1 \times \cdots \times T^{n_o}\}, \tag{10}$$

which can be easily proved by examining the definitions of cut/tie sets and those two set operations. The reliability can be calculated based on $\mathbf{C}$ or $\mathbf{T}$. This method offers flexibility when evaluating reliability under various objectives, which can be implemented as a recursive procedure when control objectives changes.

F. Searching process for cut/tie sets

There are two approaches, namely simulation based and model based approaches. If the control objectives are given in the form of transient characteristics, we can search for the cut/tie sets through the off-line simulation. If the control objectives are given that are related or can be mapped to the system models (parameters), one can find the sets by examining the system characteristics from the system models. In fact, this is the philosophy behind the control system analysis. The main procedure is given as follows.

1. Transform the system into the standard set up.
2. For all expected failure scenarios, i.e. all possible combinations of basic failures, evaluate if the objective sets are satisfied by simulation or analyzing the system models.
3. Find all the set of basic events $v_i = \{f_{i1}, \cdots, f_{in_{vi}}\}$, $w_i = \{f_{i1}, \cdots, f_{in_{wi}}\}$ such that under intersection of failure events $\bigcap_{j=1}^{n_{vi}} f_{ij}$ system fails and under the intersection of failure events $\bigcap_{j=1}^{n_{wi}} \bar{f}_{ij}$ system succeeds. Denote the set of v_i as V, and the complement of w_i in the failure set F as $\bar{w}_i$, and the set of $\bar{w}_i$ as $\overline{W}$.
4. Cut sets $\mathbf{C}$ = compact(V) and tie sets $\mathbf{T}$ = compact$(\overline{W})$, which can be easily shown by examining the previous definitions.

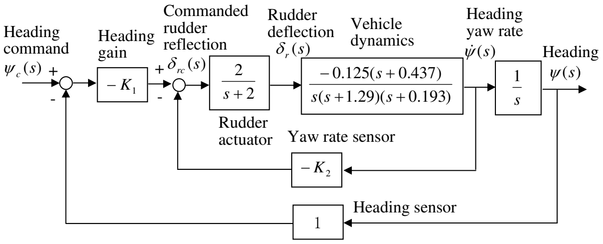

Fig. 7. Heading control for an unmanned submersible vehicle.

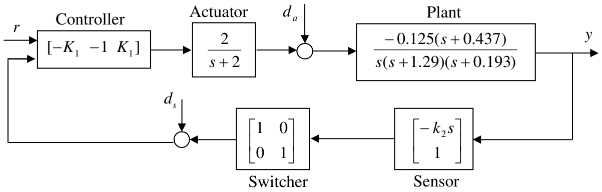
Controller
r
$[-K_1 \ -1 \ K_1]$
Actuator
$\frac{2}{s+2}$
d_a
Plant
$\frac{-0.125(s+0.437)}{s(s+1.29)(s+0.193)}$
y
d_s
$\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}$
Switcher
$\begin{bmatrix}-k_2 s\\1\end{bmatrix}$
Sensor

Fig. 8. Standard setup for the heading control system.

IV. Example

Consider a simple control system for an unmanned free-swimming submersible vehicle and the block diagram is given in Fig. IV [8]. There are two control loops in such a system, i.e., the yaw rate and heading control loop respectively, where two sensors measure the heading angle and yaw rate. First, reconfigure this system into the standard setup as shown in Fig. IV.

This system has two sensors and one actuators with the following fault scenarios:

1) Constant bias of the actuator or sensors: the value is 0.5 and the probability is 0.05.
2) Stuck of the yaw rate sensor or heading sensor: stuck at 0.5 and the probability is 0.02.

Denote the bias in actuator as f_a, the bias and stuck in the heading sensor and yaw rate sensor as f_{h1}, f_{h2}, f_{y1} and f_{y2}. The control objectives are defined as follows:

1) O_1: stable.
2) O_2: static error < 0.2.
3) O_3: settling time < 15.
4) O_4: rise time < 4.
5) O_5: overshoot < 0.5.

Then apply the two approaches to evaluate the reliability of the system under different loop gains: $K_1 = K_2 = 5$ or $K_1 = K_2 = 10$. By simulation of step response, and checking each objective for various failure scenarios, it is not hard to find out the tie sets of failure scenarios under which the system satisfies the objectives. The simulation results are given in Table 1 and 2.

However, the simulation based approach is time-consuming especially when considering all possible fault scenarios. In some cases, it is possible to map the objectives to the system parameters. For example, a system pole region

Table 1. Simulation result when K_1=K_2=5.

failure Scenario	System Succeed	Stable?	Static error	Transient characteristics		
				Settling time	Rise time	overshoot
Normal	Y	Y	0	11.64	2.92	0.1005
f_{h1}		Y	-0.5	11.64	2.90	0.1005
f_{h2}		N				
$f_{y1} \cap f_{h0}$	Y	Y	0.1	11.64	2.90	0.1005
$f_{y1} \cap f_{h1}$		Y	-0.4	11.64	2.90	0.1005
$f_{y1} \cap f_{h2}$		N				
$f_{y2} \cap f_{h0}$	Y	Y	0.1	18.66	2.10	0.3970
$f_{y2} \cap f_{h1}$		Y	-0.4	18.66	2.12	0.3970
$f_{y2} \cap f_{h2}$		N				
f_a	Y	Y	-0.1	11.68	2.90	0.1006
$f_a \cap f_{h1}$		Y	-0.6	11.76	2.88	0.1007
$f_a \cap f_{h2}$		N				
$f_a \cap f_{y1} \cap f_{h0}$	Y	Y	-0.1	11.68	2.90	0.1006
$f_a \cap f_{y1} \cap f_{h1}$		Y	-0.6	11.76	2.88	0.1007
$f_a \cap f_{y1} \cap f_{h2}$		N				
$f_a \cap f_{y2} \cap f_{h0}$	Y	Y	0	18.7	2.10	0.3972
$f_a \cap f_{y2} \cap f_{h1}$		Y	-0.5	18.76	2.10	0.3977
$f_a \cap f_{y2} \cap f_{h2}$		N				

Table 2. Simulation result when K_1=K_2=10.

failure Scenario	System Succeed	Stable?	Static error	Transient characteristics		
				Settling time	Rise time	overshoot
Normal	Y	Y	0	8.12	1.98	0.0669
f_{h1}		Y	-0.5	8.12	1.98	0.0669
f_{h2}		N				
f_{y1}	Y	Y	0.05	8.12	1.98	0.0669
$f_{y1} \cap f_{h1}$		Y	-0.45	8.12	2	0.669
$f_{y1} \cap f_{h2}$		N				
f_{y2}		Y	0.05	22.54	1.34	0.6171
$f_{y2} \cap f_{h1}$		Y	-0.45	22.54	1.36	0.6171
$f_{y2} \cap f_{h2}$		N				
f_a	Y	Y	-0.05	8.14	1.98	0.0669
$f_a \cap f_{h1}$		Y	-0.55	8.16	0.98	0.0670
$f_a \cap f_{h2}$		N				
$f_a \cap f_{y1}$	Y	Y	0	8.14	2	0.0669
$f_a \cap f_{y1} \cap f_{h1}$		Y	-0.5	8.16	0.98	0.0670
$f_a \cap f_{y1} \cap f_{h2}$		N				
$f_a \cap f_{y2}$		Y	0	22.56	1.36	0.6173
$f_a \cap f_{y2} \cap f_{h1}$		Y	-0.5	22.58	1.36	0.6177
$f_a \cap f_{y2} \cap f_{h2}$		N				

can be used to characterize performance requirements and mapped to a region in the parametric space [9]. In this example, the performance requirement can be specified by the pole region of the closed-loop system given in Fig. IV. So the objectives can be restated as:

1) O'_1: all the poles have real parts less than -0.1.
2) O'_2: the tangent of the angle between the poles and the real axis is less than 4.5.
3) O'_3: $\mid lim_{s\to 0} s(G_{da}(s)d_a(s) + G_{ds}(s)d_s(s)) \mid < 0.2$.

It is not hard to program in MATLAB to check these requirements automatically. Then by checking these model-related requirements for each failure scenario, we can easily find the following tie sets:

- When $K_1 = K_2 = 5$, the tie set is $\{f_{h1}, f_{h2}.\}$.
- When $K_1 = K_2 = 10$, the tie set is $\{f_{h1}, f_{h2}, f_{y2}.\}$.

As we can see, when the loop gains changes, the tie set also changes and the reliability of the system is not the same. So the reliability of the system can be computed as:

- When $K_1 = K_2 = 5$, $R = \Pr\{\overline{f}_{h1} \cap \overline{f}_{h2}\} = 0.931$.
- When $K_1 = K_2 = 10$, $R = \Pr\{\overline{f}_{h1} \cap \overline{f}_{h2} \cap \overline{f}_{y2}\} = 0.9123$.

If f_{y2} is detected with false alarm probability 0.1, the occurrence probability of f_{y2} is updated as 0.9. If $K_1 = K_2 = 5$, the reliability remain unchanged but it decreases to 0.0931 if $K_1 = K_2 = 10$. For this particular system, when decreasing the loop gains, the reliability is improved. This example demonstrates that the reliability of the control system not only depends on the redundancy in the system but also the controller. This is consistent with the design philosophy of the fault tolerant control system which attempts to improve the reliability by a control means.

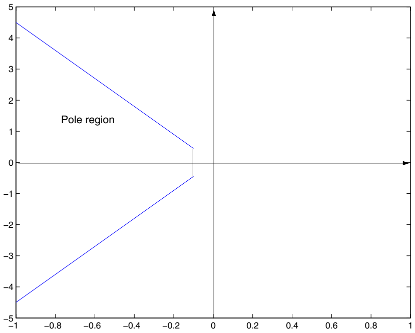

Fig. 9. Pole region for the performance objectives.

V. Concluding Comments

This work provides a preliminary study on reliability evaluation of control systems. The method is based on the equivalent cut/tie set of a control system, based on which the reliability is calculated. Furthermore, when control objective set changes or some failures are detected, the cut/tie set and reliability evaluation can be updated. In the case of a large-scale system with a lot of control loops and components, we may decompose it into subsystems and apply the evaluation method on them; then calculate the reliability of the system based on subsystem radiabilities. One simple example is provided to illustrate the method and it shows that better reliability in a control system can be achieved by proper controller design. So it is indeed possible to guide the design of a control system according to the reliability requirement.

References

[1] N. Wu. "Coverage in fault-tolerant control", *Automatica*, vol. 40, no. 4, pp. 537-548, 2004.

[2] M. Blanke, M. Staroswiecki and N. Wu. "Concepts and methods in fault-tolerant control", *Proc. American Contr. Conf.*, Arlington, USA, 2001, pp. 2606-2620.

[3] H. Kumanmoto, E. Henley and K. Inoue. "Signal-flow-based graphs for failure-mode analysis of systems with control Loops", *IEEE Trans. Reliability*, vol. 30, no. 2, 1981.

[4] N. Viswanadham, V. Sarma and M. Singh. *Reliability of Computer and Control Systems*, Elsevier Science Pubilishers, Amsterdam, 1987.

[5] M. Galluzzo & P. Andow, "Reliability Analysis of Systems Containing Complex Control Loops", *Reliability of Instrumentation Systems for Safeguarding and Control*, edited by J. Jansen & L. Boullart, Proc. IFAC Workshop, Hague, Netherlands, May 1986, pp. 47-52.

[6] P. Wasiewicz, "Method for comparison of computer control system structures in the functional reliability aspect", *Reliability of Instrumentation Systems for Safeguarding and Control*, edited by J. Jansen & L. Boullart, Proc. IFAC Workshop, Hague, Netherlands, May 1986, pp. 55-60.

[7] R. Billinton and R. Allan. *Reliability evaluation of engineering systems*, Plenum Press, Marshfield, 1983.

[8] N. Nise, *Control Systems Engineering*, Addison-Wesley Publishing Company, Menlo Park, 1995.

[9] J. Ackermann. *Robust Control*, Springer-Verlag, London, 2002.