A&QT-R 2002 (THETA 13)

2002 IEEE-TTTC-International Conference on Automation, Quality and Testing, Robotics

May 23 – 25, 2002, Cluj-Napoca, Romania

FAILURE MODE EFFECTS AND TESTABILITY ANALYSES OF ELECTRONIC SYSTEMS FOR CRITICAL APPLICATIONS

Assist. Prof. Mihaela Radu, Ph.D.
Dipl. Eng. Cristian Posteuca
Dipl. Eng. Neta Habermann

Technical University of Cluj-Napoca
IPA –R@D Institute for Automation, Cluj Napoca
BQR, Reliability Eng. Ltd.,Rishon-Lezion,Israel

Abstract: In critical-computation applications the incorrect performance of the system will almost certainly yield devastating results. Typical examples include aircraft flight control systems, space shuttle. The crucial areas of applications drastically require ultra-reliable digital systems, forcing the designers and manufactures to find new ways to improve the dependability (the confidence degree) of electronic systems.

For an electronic system used in critical applications, it is extremely important in the design process to perform a Failure Mode Effects Analysis (FMEA), possible combined with a Criticality Analysis (FMECA), followed by Testability Analysis (TA), in addition to the well-known reliability evaluations.

This article presents FMECA and TA estimation for a flight controller that is performed using CARE analysis tools. CARE is an engineering tool, developed by BQR Reliability Ltd., which can be used concurrently in the phases of Research & Development, Reliability Analyses and Testing of a new product. This article is the output of a scientific co-operation with BQR Reliability Eng. Ltd., Israel, concerning detailed reliability evaluations of electronic systems.

Keywords: critical application, failure effect, testability

1. INTRODUCTION

Nowadays, digital systems, especially computers are incorporated into aircraft flight control systems, industrial controllers, banking networks. In each application, erroneous results or failures of the system can be dangerous to human life, environmental protection and financial record [3]. These applications are called critical applications, because the incorrect performance of the system can jeopardize human safety, environmental cleanliness, financial records. The vast and crucial areas of such applications drastically require ultra-reliable digital systems, forcing the designers and manufactures to find new ways to improve the dependability of digital systems.

For an electronic system used in critical applications, it is extremely important in the design process to perform a Failure Mode Effects Analysis (FMEA), possible combined with a Criticality Analysis (FMECA), followed by Testability Analysis (TA), in addition to the classical reliability evaluations.

This paper is organized as follows. In paragraph 1.1 we present the system, FMECA and TA concepts are presented in paragraphs 1.2 and 1.3 and FMECA and TA estimations using CARE tools are presented in section 2. Section 3 summarizes the results.

CARE is an engineering tool, developed by BQR Reliability Ltd., Israel that can be used concurrently in the phases of R&D, Reliability Analyses and Testing of a new product. This article is the output of a scientific co-operation with the above-mentioned company, in 2000-2001, concerning reliability evaluations of electronic systems.

1.1. Architecture of a Flight Control System

A system used in a critical-computation application is the architecture of a flight control system. For this system a high reliability is required during a required mission time (the “so-called” ultra-reliable or highly dependable systems).

An electronic system samples the position of the pilot’s stick, calculates the desired position of the control surfaces and commands a motor to move the control surfaces. The control system uses three identical computers performing the same operations (triple modular redundancy). The results from each computer are examined, and the output from the system is formed via a majority vote of the three results. Consequently, the two computers that are performing correctly will overrule a single computer performing incorrectly. The schematic block of the flight control system is presented in figure 1 and the corresponding functions of the blocks are:

-Sensors – get information about the position of the pilot’s stick,

-Cockpit Controls and Displays – pilot’s control and display facilities,

-Processors 1, 2, 3 (combined in a triple modular redundancy) – calculate the desired position of the control surfaces,

-Voter – computes the majority function for the results of the processors,

-Control Surface Actuators – command a motor to move the control surfaces (for example ailerons, elevators and rudder).

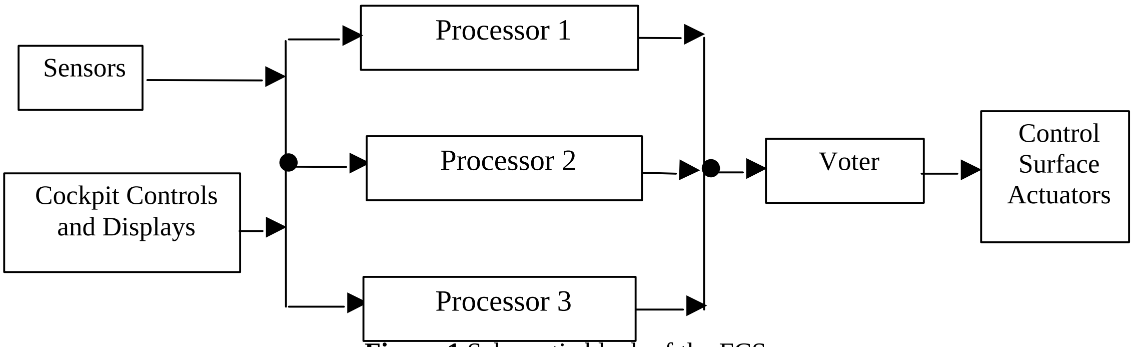


Figure 1 Schematic block of the FCS

Each functional block contains sub-blocks and components, detailed in the reliability block tree [8]. The processors are Motorola 68360 processors from CARE main library and the voting structure uses CMOS logic gates, the HC 74xxx family. In addition to the reliability estimations, which are performed using RBD module of CARE software, it is essential for these systems to perform FMEA and/or FMECA analyses, followed by a Testability Analysis.

1.2. FMEA analysis

FMEA analysis identifies potential problems and the appropriate corrective action. These analyses are often referred to as Fault Hazard Analysis (FHA), Criticality Analysis, Risk Analysis, Failure Modes and Criticality Analysis (FMECA) [2]. FMECA serves as a dictionary of failure modes for safety and logistics analysis. The FMECA results serve as the main input to define Built in Tests (BIT) that can automatically detect and isolate system failures as they occur, consequently increasing the system availability [1], [2]. The purpose is:

- To analyze the end effects at the system level caused by each component failure,
- Vice versa: to describe all possible causes of each end effect,
- To calculate every end effect rate and each failure criticality,
- To define each failure severity,
- To define which failures are the most emergent considering their severity and probability.

We suggest o possible way to plan FMEA:

Table 1

Planning the FMEA		
Failure Modes	Effects	Causes
Occurrence	Severity	Detection
Interpretation		
The Follow Through (Preventive and/or Corrective Action)		

1.3 Testability Analysis and Testing Procedures

After modeling the possible defects of the circuit, testing procedures to cover these defects have to be established. An extremely important part of the design process is the development of a plan for testing the resulting designs and the actual testing itself.

Testing involves searching for faults of all types, including faults resulting from design mistakes, implementation mistakes and component defects. The overall purpose of the test phase in the design process is to ensure the correct operation of the system. Testing of digital systems or a single circuit but in a critical position is extremely vital to the ultimate goal of achieving high reliability, availability, safety, maintainability, or other design requirements.

Test procedures can be performed using two major approaches: external test and built-in test. External test techniques usually require that the device under test is removed from its operational environment and subjected to various tests using equipment that is external to the device (ATE procedures). Built-in test techniques are usually incorporated into the design of the device such that testing can be performed without the need of external test equipment.

Regardless of whether the test capability is external or built-in, there are three major types of tests recommended for logic circuits.

The first type of test is called functional test. Functional testing attempts to verify that the Device Under Test (DUT) possesses the functional characteristics that it was intended to have. The second type of test is called parametric test. The purpose of this test is to verify that certain parameters of the DUT such as voltages, currents are within the required ranges. The third type of test is the dynamic test. This type of testing checks the switching time of logic gates, propagation delays, to confirm that they are acceptable.

2. FAILURE MODE EFFECTS AND TESTABILITY ANALYSES FOR A FLIGHT CONTROLLER

2.1 Reliability specifications

For this system the reliability specifications are:

- The Flight Control System must continuously operate 3hours/day.
- It is installed on Airborne, Inhabited, Cargo, into an aeroplane.
- The required MTBF is 25.000 hours.

For Reliability predictions the S217F2-Part Stress standard is used [1]. A typical requirement for a critical-computation application is to have a reliability of 0.9999999 (0.9_7) at the end of a three-hour period.

2.2 FMECA (Failure Mode Effect and Criticality Analysis)

The FMECA module from CARE software is used to analyze system's assemblies failure modes effects on the overall system functionality. FMECA is performed using the functional tree of the system. This tree represents the signals/data flow from the lowest level functional block up to the higher level functional blocks. For each component of the system, an internal cause, effects and failure modes are defined, building the system's tree of failure modes and effects.

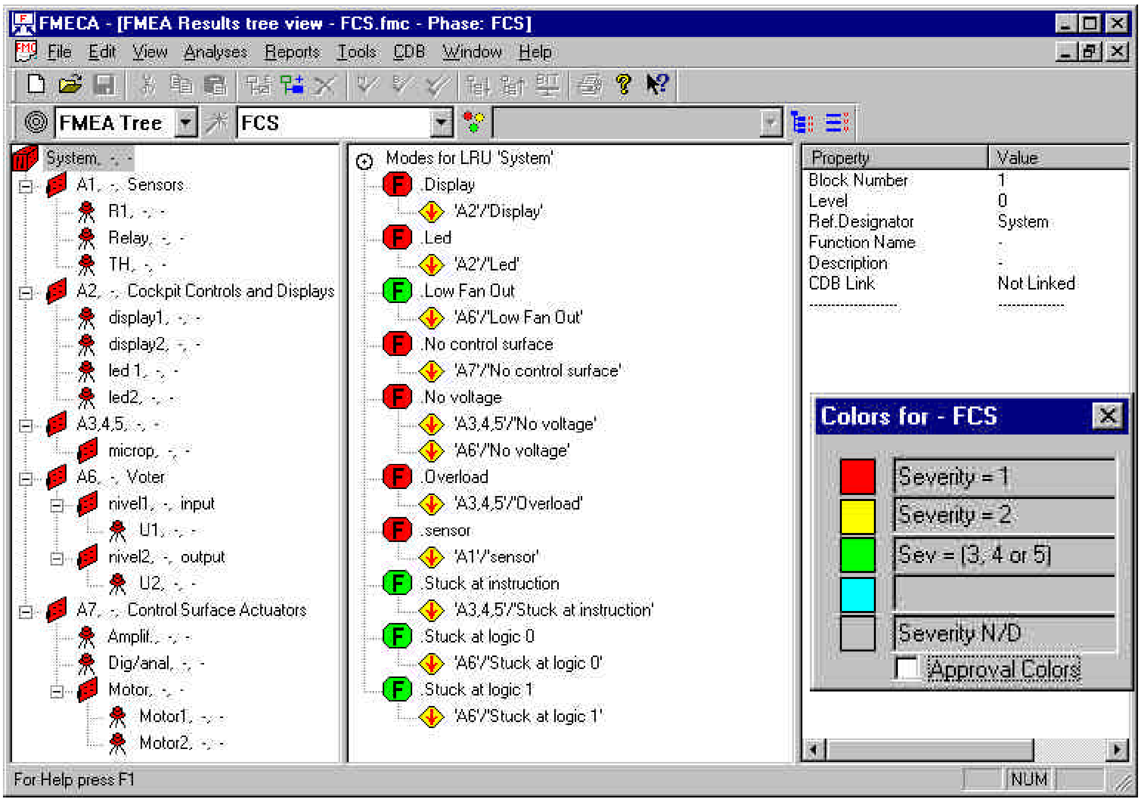
The CARE software allocates the severity for the end effects of the failures of components and calculates their criticality. **End Effect Severity** is the emergency measure of the end effect. The default severity values are **I –catastrophic, II – critical, III – marginal (or major), IV – minor [1]**. CARE FMECA allows 2 types of Criticality Matrix Ranks: MIL-STD-1629A and Pareto ranking with additional control possibilities for the user. Both methods are based on **Criticality Matrix**. See figure 2:

Probability ranking groups	Severity				
	V	IV	III	II	I
0.2 – 1					
0.1 – 0.2					1
0.01 – 0.1			4	2	1
0.001 – 0.01					
0 – 0.001			1		1

Figure 2 Criticality Matrix

Criticality Matrix is the **End Effect Probability – Severity table** with the numbers of the system **internal causes** located in each cell, that is having the corresponding end effect probability and severity. Ranking is the method to assign an emergency qualitative measure for each cell having internal causes [1].

In figure 3 the results of the FMEA analysis is presented and in figure 4 the results of the Criticality Analysis (which failures are the most emergent). According to the severity ranking of the possible failures of components, the program calculates the unsafe regions for the system.


FMECA - [FMEA Results tree view - FCS.fmc - Phase: FCS]
File Edit View Analyses Reports Tools CDB Window Help
FMEA Tree
FCS
For Help press F1
NUM

```
System, -, -
  A1, -, Sensors
    R1, -, -
    Relay, -, -
    TH, -, -
  A2, -, Cockpit Controls and Displays
    display1, -, -
    display2, -, -
    led 1, -, -
    led2, -, -
  A3,4,5, -, -
    microp, -, -
  A6, -, Voter
    nivel1, -, input
      U1, -, -
    nivel2, -, output
      U2, -, -
  A7, -, Control Surface Actuators
    Amplif., -, -
    Dig/anal, -, -
    Motor, -, -
      Motor1, -, -
      Motor2, -, -
```

```
Modes for LRU 'System'
  .Display
    'A2'/'Display'
  .Led
    'A2'/'Led'
  .Low Fan Out
    'A6'/'Low Fan Out'
  .No control surface
    'A7'/'No control surface'
  .No voltage
    'A3,4,5'/'No voltage'
    'A6'/'No voltage'
  .Overload
    'A3,4,5'/'Overload'
  .sensor
    'A1'/'sensor'
  .Stuck at instruction
    'A3,4,5'/'Stuck at instruction'
  .Stuck at logic 0
    'A6'/'Stuck at logic 0'
  .Stuck at logic 1
    'A6'/'Stuck at logic 1'
```

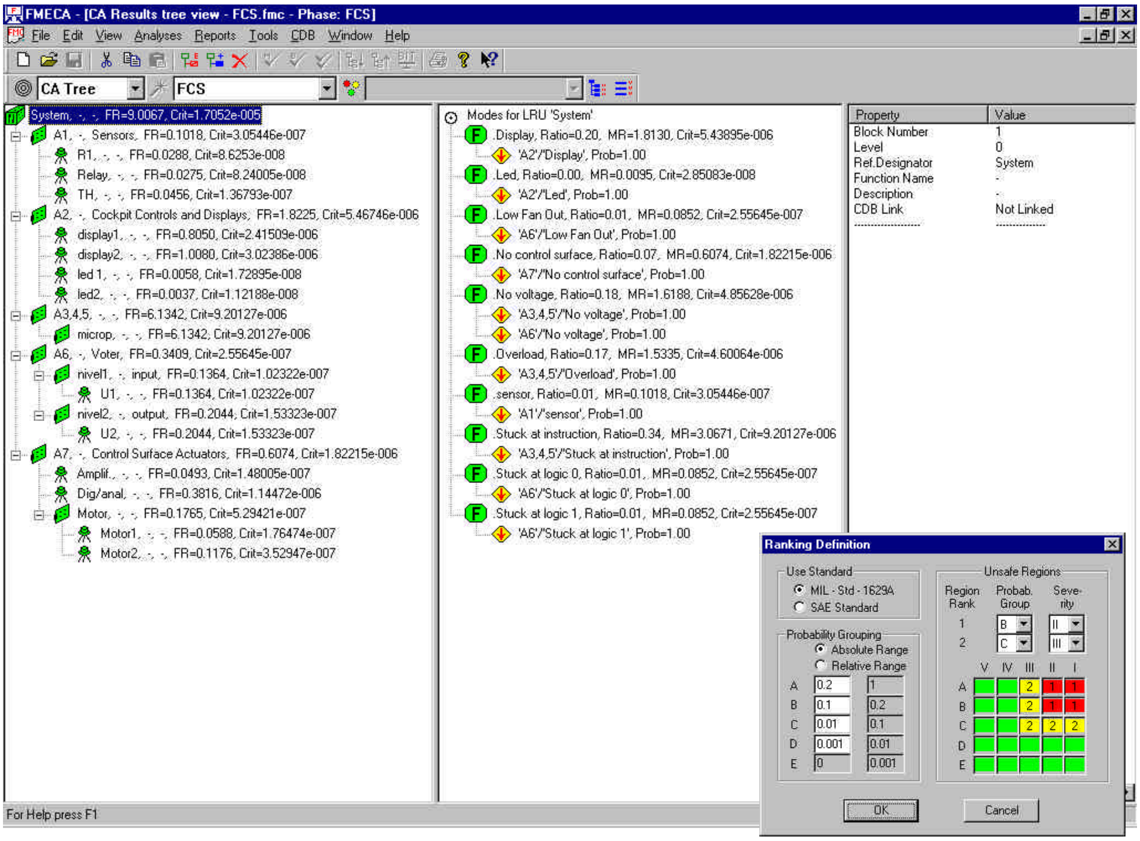
Property	Value
Block Number	1
Level	0
Ref.Designator	System
Function Name	-
Description	-
CDB Link	Not Linked

Colors for - FCS

🟥	Severity = 1
🟨	Severity = 2
🟩	Sev = {3, 4 or 5}
🟦	
□	Severity N/D

□ Approval Colors

Figure 3 FMEA analysis for FCS


FMECA - [CA Results tree view - FCS.fmc - Phase: FCS]
File Edit View Analyses Reports Tools CDB Window Help
CA Tree
FCS
For Help press F1
OK
Cancel

```
System, -, -, FR=9.0067, Crit=1.7052e-005
  A1, -, Sensors, FR=0.1018, Crit=3.05446e-007
    R1, -, -, FR=0.0288, Crit=8.6253e-008
    Relay, -, -, FR=0.0275, Crit=8.24005e-008
    TH, -, -, FR=0.0456, Crit=1.36793e-007
  A2, -, Cockpit Controls and Displays, FR=1.8225, Crit=5.46746e-006
    display1, -, -, FR=0.8050, Crit=2.41509e-006
    display2, -, -, FR=1.0080, Crit=3.02386e-006
    led 1, -, -, FR=0.0058, Crit=1.72895e-008
    led2, -, -, FR=0.0037, Crit=1.12188e-008
  A3,4,5, -, -, FR=6.1342, Crit=9.20127e-006
    microp, -, -, FR=6.1342, Crit=9.20127e-006
  A6, -, Voter, FR=0.3409, Crit=2.55645e-007
    nivel1, -, input, FR=0.1364, Crit=1.02322e-007
      U1, -, -, FR=0.1364, Crit=1.02322e-007
    nivel2, -, output, FR=0.2044, Crit=1.53323e-007
      U2, -, -, FR=0.2044, Crit=1.53323e-007
  A7, -, Control Surface Actuators, FR=0.6074, Crit=1.82215e-006
    Amplif., -, -, FR=0.0493, Crit=1.48005e-007
    Dig/anal, -, -, FR=0.3816, Crit=1.14472e-006
    Motor, -, -, FR=0.1765, Crit=5.29421e-007
      Motor1, -, -, FR=0.0588, Crit=1.76474e-007
      Motor2, -, -, FR=0.1176, Crit=3.52947e-007
```

```
Modes for LRU 'System'
  .Display, Ratio=0.20, MR=1.8130, Crit=5.43895e-006
    'A2'/'Display', Prob=1.00
  .Led, Ratio=0.00, MR=0.0095, Crit=2.85083e-008
    'A2'/'Led', Prob=1.00
  .Low Fan Out, Ratio=0.01, MR=0.0852, Crit=2.55645e-007
    'A6'/'Low Fan Out', Prob=1.00
  .No control surface, Ratio=0.07, MR=0.6074, Crit=1.82215e-006
    'A7'/'No control surface', Prob=1.00
  .No voltage, Ratio=0.18, MR=1.6188, Crit=4.85628e-006
    'A3,4,5'/'No voltage', Prob=1.00
    'A6'/'No voltage', Prob=1.00
  .Overload, Ratio=0.17, MR=1.5335, Crit=4.60064e-006
    'A3,4,5'/'Overload', Prob=1.00
  .sensor, Ratio=0.01, MR=0.1018, Crit=3.05446e-007
    'A1'/'sensor', Prob=1.00
  .Stuck at instruction, Ratio=0.34, MR=3.0671, Crit=9.20127e-006
    'A3,4,5'/'Stuck at instruction', Prob=1.00
  .Stuck at logic 0, Ratio=0.01, MR=0.0852, Crit=2.55645e-007
    'A6'/'Stuck at logic 0', Prob=1.00
  .Stuck at logic 1, Ratio=0.01, MR=0.0852, Crit=2.55645e-007
    'A6'/'Stuck at logic 1', Prob=1.00
```

Property	Value
Block Number	1
Level	0
Ref.Designator	System
Function Name	-
Description	-
CDB Link	Not Linked

Ranking Definition

Use Standard
● MIL - Std - 1629A
○ SAE Standard

Probability Grouping
● Absolute Range
○ Relative Range

A	0.2	1
B	0.1	0.2
C	0.01	0.1
D	0.001	0.01
E	0	0.001

Unsafe Regions

Region Rank	Probab. Group	Seve-rity
1	B	II
2	C	III

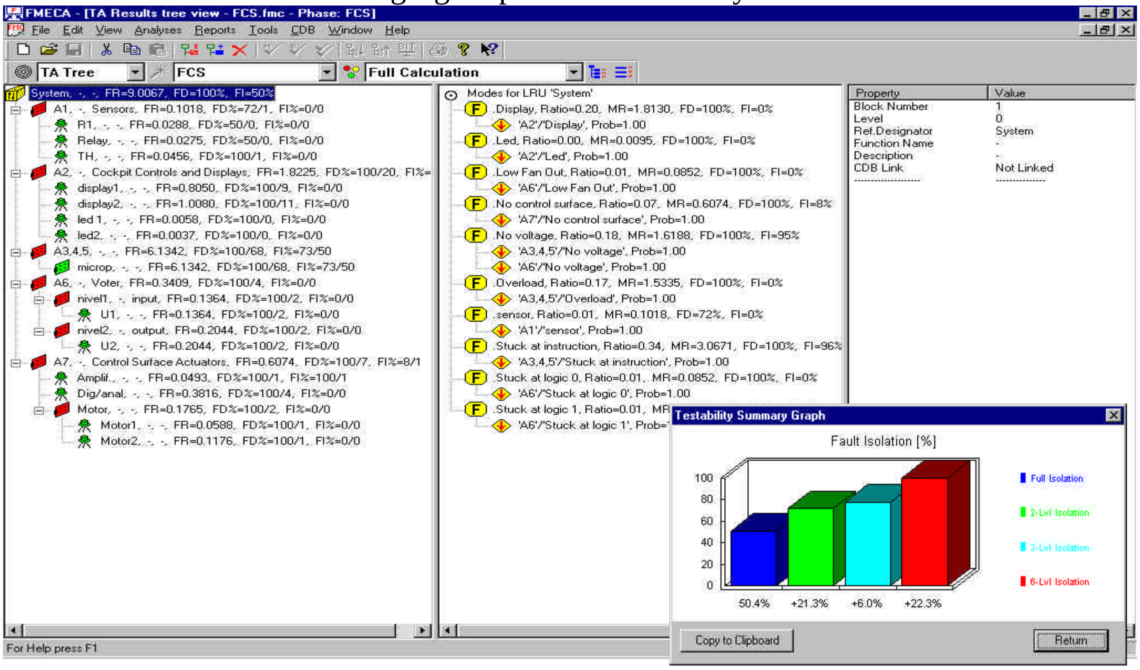
	V	IV	III	II	I
A	🟩	🟩	2	1	1
B	🟩	🟩	2	1	1
C	🟩	🟩	2	2	2
D	🟩	🟩	🟩	🟩	🟩
E	🟩	🟩	🟩	🟩	🟩

Figure 4 CA analysis for FCS

2.2 Testability Analysis

For our project "Flight Control System" we configured possible BIT tests for the microprocessors and ATE tests for the other modules. A certain defect is 100% isolated if it is detected after one testing procedure. The level of isolation decreases if more than one test is necessary to detect a certain fault.

A possible sequence of BIT (Built In Test) for microprocessor block is: Program Counter Test, Scratchpad Memory Test, Stack Pointer and Index Register Test, ALU Test, Control Lines and other Peripheral Circuits Test. ATE (Automatic Test Equipment) for other modules: Parametric Tests, Functional Tests. Dynamic Tests Power On Tests. The following figure presents Testability estimations for the FCS.



```
System, -, -, FR=9.0067, FD=100%, FI=50%
  A1, -, Sensors, FR=0.1018, FD%=72/1, FI%=0/0
    R1, -, -, FR=0.0288, FD%=50/0, FI%=0/0
    Relay, -, -, FR=0.0275, FD%=50/0, FI%=0/0
    TH, -, -, FR=0.0456, FD%=100/1, FI%=0/0
  A2, -, Cockpit Controls and Displays, FR=1.8225, FD%=100/20, FI%=
    display1, -, -, FR=0.8050, FD%=100/9, FI%=0/0
    display2, -, -, FR=1.0080, FD%=100/11, FI%=0/0
    led 1, -, -, FR=0.0058, FD%=100/0, FI%=0/0
    led2, -, -, FR=0.0037, FD%=100/0, FI%=0/0
  A3,4,5, -, -, FR=6.1342, FD%=100/68, FI%=73/50
    microp, -, -, FR=6.1342, FD%=100/68, FI%=73/50
  A6, -, Voter, FR=0.3409, FD%=100/4, FI%=0/0
    nivel1, -, input, FR=0.1364, FD%=100/2, FI%=0/0
      U1, -, -, FR=0.1364, FD%=100/2, FI%=0/0
    nivel2, -, output, FR=0.2044, FD%=100/2, FI%=0/0
      U2, -, -, FR=0.2044, FD%=100/2, FI%=0/0
  A7, -, Control Surface Actuators, FR=0.6074, FD%=100/7, FI%=8/1
    Amplif., -, -, FR=0.0493, FD%=100/1, FI%=100/1
    Dig/anal, -, -, FR=0.3816, FD%=100/4, FI%=0/0
    Motor, -, -, FR=0.1765, FD%=100/2, FI%=0/0
      Motor1, -, -, FR=0.0588, FD%=100/1, FI%=0/0
      Motor2, -, -, FR=0.1176, FD%=100/1, FI%=0/0
```

```
Modes for LRU 'System'
  F .Display, Ratio=0.20, MR=1.8130, FD=100%, FI=0%
      'A2'/'Display', Prob=1.00
  F .Led, Ratio=0.00, MR=0.0095, FD=100%, FI=0%
      'A2'/'Led', Prob=1.00
  F .Low Fan Out, Ratio=0.01, MR=0.0852, FD=100%, FI=0%
      'A6'/'Low Fan Out', Prob=1.00
  F .No control surface, Ratio=0.07, MR=0.6074, FD=100%, FI=8%
      'A7'/'No control surface', Prob=1.00
  F .No voltage, Ratio=0.18, MR=1.6188, FD=100%, FI=95%
      'A3,4,5'/'No voltage', Prob=1.00
      'A6'/'No voltage', Prob=1.00
  F .Overload, Ratio=0.17, MR=1.5335, FD=100%, FI=0%
      'A3,4,5'/'Overload', Prob=1.00
  F .sensor, Ratio=0.01, MR=0.1018, FD=72%, FI=0%
      'A1'/'sensor', Prob=1.00
  F .Stuck at instruction, Ratio=0.34, MR=3.0671, FD=100%, FI=96%
      'A3,4,5'/'Stuck at instruction', Prob=1.00
  F .Stuck at logic 0, Ratio=0.01, MR=0.0852, FD=100%, FI=0%
      'A6'/'Stuck at logic 0', Prob=1.00
  F .Stuck at logic 1, Ratio=0.01, MR
      'A6'/'Stuck at logic 1', Prob=
```

Property	Value
Block Number	1
Level	0
Ref.Designator	System
Function Name	-
Description	-
CDB Link	Not Linked

Figure 5 TA analysis for FCS

3. CONCLUSIONS

This paper presented in a concise manner certain aspects of the FMECA and TA analyses for an electronic system used in critical applications. The FMECA and Testability Analyses are essential steps in design of these structures before being incorporated in the final system for safety and logistics purposes. The project presented and completed by the authors is designated to BQR's industrial customers from the area of Aviation and Aerospace.

REFERENCES

[1] BQR Reliability Engineering (2000), "CARE Basic Tutorial", version 2.2.9, Rishon-Lezion, Israel,.

[2] Y. Bot (1995) "FMECA for Software and Hardware", Proceedings of "*The Third National Conference of the Israel Society for Quality*", Tel-Aviv, Israel, pp. 344.

[3] D.K. Pradham (1996), " Fault-Tolerant Computer System Design", Prentice Hall, USA.

[4]Radu Mihaela, Posteuca C., Viman Liviu (2000), "FMEA/FMECA – Failure Mode Effects and Criticality Analysis of Fault Tolerant Systems" Proceedings of "*DAAAM 2000*", Opatjia, Croatia, pag.397-398.

[5] Radu Mihaela, Pitica Dan, Posteuca Cristian (2001)"Complex Reliability Evaluation of Voters for Fault Tolerant Designs", Proceedings of "*IEEE-ISQED 2001, International Symposium on Quality of Electronic Design*", San Jose, California, USA, pag. 331-337.

[6] Mihaela Radu, Munteanu Radu (2000) "Testability Analysis of Voting Networks", Proceedings of "*SIITME 2000, International Seminar for Informatics and Technology in Electronic Modules*" Polytechnic Institute, Bucharest.

[7] Mihaela Radu, Posteuca C., Neta Habermann (2001) "CARE Tutorials. User's manual", www.bqr.com.