Developing a rigorous bottom-up modular static failure modelling methodology

R.Clark* , A. Fish† , C. Garrett†, J. Howse†
*Energy Technology Control, UK. r.clark@energytechnologycontrol.com
†University of Brighton, UK

Keywords: static failure mode modelling safety-critical

Abstract

The certification process of safety critical products for European and other international standards often demand environmental stress, endurance and Electro Magnetic Compatibility (EMC) testing. Theoretical, or 'static testing', is often also required. In general static testing will reveal modifications that must be made to improve the product safety, or identify theoretical weaknesses in the design. This paper proposes a new theoretical methodology for creating failure mode models of systems. It has a common notation for mechanical, electronic and software domains and is modular and hierarchical. The method provides advantages in rigour and efficiency when compared to current methodologies.

1 Introduction

This paper describes and appraises four current failure modelling methodologies. Their advantages and deficiencies are discussed and a desirable criteria list for an 'ideal' static failure mode methodology is developed. A proposed methodology is then described. A worked example is then presented, using the new methodology, which models the failure mode behaviour of a non-inverting op-amp circuit. Using the worked example the new methodology is evaluated. Finally the desirable criteria list is presented as a check box table alongside four current methodologies.

We briefly analyse four current methodologies. Comprehensive overviews of these methodologies may be found in [5, 11].

Fault Tree Analysis (FTA). FTA [6, 8] is a top down methodology in which a hierarchical diagram is drawn for each undesirable top level failure/event, presenting the conditions that must arise to cause the event. It is suitable for large complicated systems with few undesirable top level failures and focuses on those events considered most important or most catastrophic. Effects of duplication/redundancy of safety systems can be readily assessed. It uses notations that are readily understood by engineers (logic symbols borrowed from digital electronics and a fault hierarchy). However, it cannot guarantee to model all base component failures or be used to determine system level errors other than those modelled. Each FTA diagram models one top level event. This creates duplication of modelled elements, and it is difficult to cross check between diagrams. It has limited support for environmental and operational states.

Fault Mode Effects Analysis (FMEA) is used principally to determine system reliability. It is bottom-up and starts with component failure modes, which lead to top level failure/events. Each top level failure is assessed by its cost to repair (or perceived criticality) and its estimated frequency. A list of failures according to their cost to repair [4], or effect on system reliability is then calculated. It is easy to identify single component failure to system failure mappings and an estimate of product reliability can be calculated. It cannot focus on complex component interactions that cause system failure modes or determine potential problems from simultaneous failures. It does not consider changing environmental or operational states in sub-systems or components. It cannot model self-checking safety elements or other in-built safety features or analyse how particular components may fail.

Failure Mode Effects Criticality Analysis (FMECA) is a refinement of FMEA, using extra variables: the probability of a component failure mode

occurring, the probability that this will cause a given top level failure, and the perceived criticality. It gives better estimations of product reliability/safety and the occurrence of particular system failure modes than FMEA but has similar deficiencies.

Failure Modes, Effects and Diagnostic Analysis (FMEDA) is a refinement of FMEA and FMECA and in addition models self-checking safety elements. It assigns two attributes to component failure modes: detectable/undetectable and safe/dangerous. Statistical measures about the system can be made and used to classify a safety integrity level. It allows designs with in-built safety features to be assessed. Otherwise, it has similar deficiencies to FMEA. However, it has limited support for environmental and operational states in sub-systems or components, via self checking statistical mitigation. FMEDA is the methodology associated with the safety integrity standards IOC5108 and EN61508 [9].

1.1 Summary of Deficiencies in Current Methods

Top Down approach: FTA The top down technique FTA, introduces the possibility of missing base component level failure modes [1][Ch.9]. Since one FTA tree is drawn for each top level event, this leads to repeated work, with limited ability for cross checking/model validation. Also, the analysis process can miss top level events that bottom-up techniques can reveal.

State Explosion problem for FMEA, FMECA, FMEDA. The bottom-up techniques all suffer from state explosion. To perform the analysis rigorously, we would need to consider the effect of a component failure against all other components. Adding environmental and operational states further increases the state explosion.

Let N be the number of components in our system, and K be the average number of component failure modes (ways in which a component can fail). The approximate total number of base component failure modes is $N \times K$. The total number of cases to examine, to determine the effect of all failure modes on all components will be approximately $(N-1) \times N \times K$. If E is the number of environmental conditions to consider in a system, and A the number of applied/operational states (or modes of the system), the bottom-up analyst is presented with two additional factors, yielding approximately $(N-1) \times N \times K \times E \times A$. If we put some typical very small embedded system numbers[1] into this, say $N = 100$, $K = 2.5$, $A = 2$, and $E = 10$ we have $99 \times 100 \times 2.5 \times 10 \times 2 = 495000$ checks to perform. To look in detail at half a million fault scenarios is obviously impractical.

2 Desirable Criteria.

From the deficiencies outlined above, we can form a set of desirable criteria for an enhanced failure mode methodology.

1. Address the state explosion problem.
2. Ensure that all component failure modes are considered in the model.
3. Be easy to integrate mechanical, electronic and software models [11][p.287].
4. Be modular, in that commonly used functional groups can be re-used in other designs/projects.
5. Have a formal basis, i.e. be able to produce mathematical traceability for its results, such as error causation trees.
6. Be able to model multiple (simultaneous) failure modes.

3 The proposed Methodology

To ensure all component failure modes are represented, the new methodology must be bottom-up. This seems essential to satisfy criterion 2. The proposed methodology is therefore a bottom-up process starting with base components. Since we are only modelling failure modes, which could arise from mechanical, electronic or software components, criterion 3 is satisfied. In order to address the state explosion problem, the process should be modular and hierarchical, dealing with small groups of components at a time; this should address criterion 1.

A *functional group*, is defined as a small collection of components that interact to provide a function or task within a system. In the proposed methodology components are collected into functional groups and each component failure (and possibly multiple simultaneous component failures) are considered in the context of the functional group.

[1] These figures would be typical of a very simple temperature controller, with a micro-controller, sensors, an RS485 interface, supporting circuitry and heater circuitry.

The component failures are termed *fault scenarios*. For each fault scenario there will be a corresponding resultant failure, or 'symptom', from the perspective of the functional group. It is conjectured that many symptoms will be common. That is to say that component failures will often cause the same symptoms of failure from the perspective of a functional group.

A common symptom collection stage is now applied. Here common symptoms are collected from the results of the fault scenarios. Because it is possible to model combinations of failures, criterion 6 is satisfied. With a collection of the functional group failure symptoms, we can create a *derived component*. The failure modes of this new derived component are the symptoms of the functional group it was derived from. This satisfies criterion 4, as we can now treat derived components as pre-analysed modules available for re-use.

By using derived components in higher level functional groups, a hierarchy can be built representing the failure mode behaviour of a system. Because the hierarchy maintains information linking the symptoms to component failure modes (via fault scenarios), we have traceable reasoning connections from base component failures to top level failures. The traceability should satisfy criterion 5.

4 Non-Inverting Amplifier

As an example, we consider a standard non-inverting op amp [7][p.234], shown in figure 1.

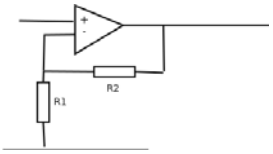

Figure 1: Standard non inverting amplifier configuration

The function of the resistors in this circuit is to set the amplifier gain. They operate as a potential divider and program the minus input on the op-amp to balance them against the positive input, giving the voltage gain (G_v) defined by $G_v = 1 + \frac{R2}{R1}$ at the output.

As the resistors work to provide a specific function, that of a potential divider, we can treat them as a functional group. This functional group has two members, $R1$ and $R2$. Using the EN298 specification for resistor failure [10][App.A], we can assign failure modes of $OPEN$ and $SHORT$ to the resistors. We represent a resistor and its failure modes as a directed acyclic graph (DAG) (see figure 2). Thus $R1$ has failure modes $\{R1\_OPEN, R1\_SHORT\}$ and $R2$ has failure modes $\{R2\_OPEN, R2\_SHORT\}$.

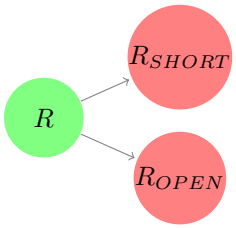

Figure 2: DAG representing a resistor and its failure modes

We look at each of these base component failure modes, and determine how they affect the operation of the potential divider.

For this example we look at single failure modes only. For each failure mode in our functional group 'potential divider' we can assign a fault scenario number (see table 1). Each fault scenario is analysed to determine the 'symptom' of the potential dividers' operation. For instance if resistor R_1 was to go open, then the circuit would not be grounded and the voltage output from it would float high (+ve). This would mean the symptom of the failed potential divider would be that it gives a high voltage output.

From table 1 we can see that the resistor failures modes lead to some common symptoms. By drawing directed edges, from the failure modes to the symptoms we can show the relationships between the component failure modes and resultant symptoms. This is represented in the DAG in figure 3.

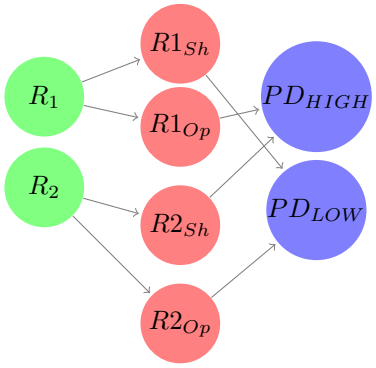

Figure 3: Failure symptoms of the 'Potential Divider'

We can now represent the potential divider as a derived component. Because we have its symptoms (or failure mode behaviour), we can treat these as the failure

Table 1: Potential Divider: Failure Mode Effects Analysis: Single Faults

Fault Scenario	**Pot.Div Effect**	**Symptom Description**
FS1: R_1 SHORT	LOW	LowPD
FS2: R_1 OPEN	HIGH	HighPD
FS3: R_2 SHORT	HIGH	HighPD
FS4: R_2 OPEN	LOW	LowPD

modes of a new derived component. We can represent this as a DAG (see figure 4).

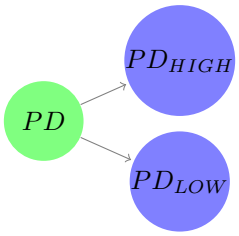

Figure 4: DAG representing a Potential Divider (PD) its failure symptoms

The derived component is defined by its failure modes and the functional group used to derive it. We now have a derived component model for a generic potential divider, and can use it as a building block for other functional groups in the same way as we used the base components $R1$ and $R2$.

Let use now consider the op-amp. According to FMD-91 [2][3-116] an op amp may have the following failure modes: latchup(12.5%), latchdown(6%), nooperation(31.3%), lowslewrate(50%). We can represent these failure modes on a DAG (see figure 5).

We can now consider merging the OP amp and the potential divider, to form a functional group to represent the non inverting amplifier. We have the failure modes of the derived component for the potential divider, so we do not need to go back and consider the individual resistor failure modes that defined its behaviour.

We can now create a functional group for the non-inverting amplifier by bringing together the failure modes from **opamp** and **PD**. Each of these failure modes will be given a fault scenario for analysis, and this is represented in table 2.

Let us consider, for the sake of the example, that the voltage follower (very low gain of 1.0) amplification characteristics from FS2 and FS6 can be considered as low output

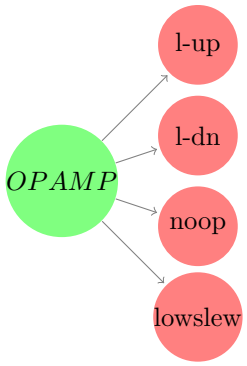

Figure 5: DAG representing failure modes of an Op-amp

Table 2: Non Inverting Amplifier: Failure Mode Effects Analysis: Single Faults

Fault Scenario	**Amplifier Effect**	**Symptom Description**
FS1: $OPAMP$ LatchUP	Output High	AMPHigh
FS2: $OPAMP$ LatchDown	Output Low Low gain	AMPLow
FS3: $OPAMP$ No Operation	Output Low	AMPLow
FS4: $OPAMP$ Low Slew	Low pass filtering	LowPass
FS5: PD LowPD	Output High	AMPHigh
FS6: PD HighPD	Output Low Low Gain	AMPLow

from the OPAMP for the application in hand (say millivolt signal amplification).

For this amplifier configuration we have three failure modes; $AMPHigh, AMPLow, LowPass$.

We can now expand the PD derived component and have a full FMMD failure model drawn as a DAG, which we can use to traverse to determine the possible causes to the three high level symptoms, i.e. the failure modes of the non-inverting amplifier. Figure 6 shows a fully expanded DAG, from which we can derive information to assist in building models for FTA, FMEA, FMECA and FMEDA failure mode analysis methodologies.

The potential divider derived component reduced the number of failures to consider from four to two. The op-amp and potential divider modelled together, reduced the number of base component failures from eight to three failure symptoms. In general, because symptoms are col-

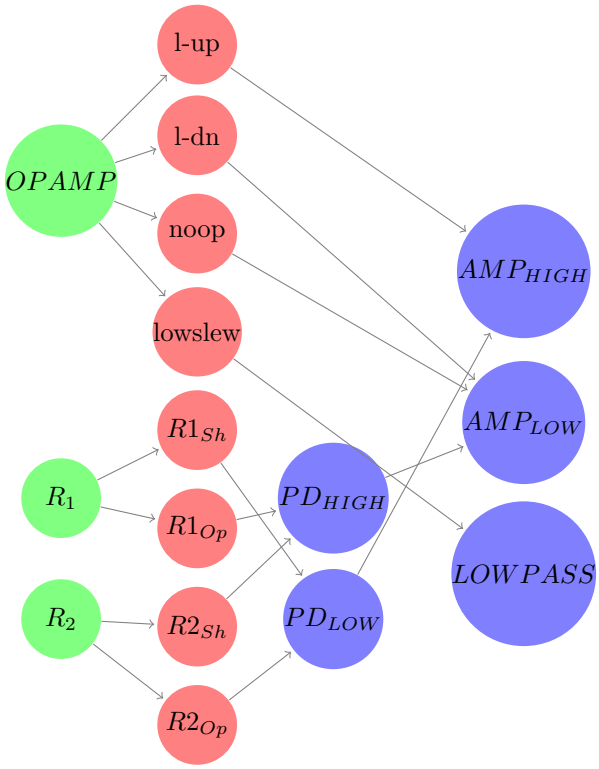

Figure 6: Full DAG representing failure modes and symptoms of the Non Inverting Op-amp Circuit

lected, we can state the number of failure symptoms for a functional group will be less than or equal to the number of component failures. This methodology has also been applied elsewhere to the inverting amplifier configuration. One can then use use derived components in more complex circuits where the advantages of FMMD become more obvious, (such as 8^{th} order filters using four bi-quad op-amp stages).

4.1 Evaluation of FMMD

We evaluate the FMMD method using the criteria in section 2. Table 3 compares the current methodologies and FMMD using these criteria.

- State explosion is reduced, because small collections of components are dealt within functional groups which are used to create derived components which are then used in an hierarchical manner.
- All component failure modes must be considered in the model. Since the proposed methodology is bottom-up, this means that we can ensure/check that all component failure modes are handled.
- It should be straightforward to integrate mechanical, electronic and software models, because FMMD models in terms of failure modes only. Because of this we can model and analyse integrated electromechanical systems, controlled by computers, using a common notation.
- It should be re-usable, in that commonly used modules can be re-used in other designs/projects. The hierarchical nature, taking functional groups and deriving components from them, means that commonly used derived components can be re-used in a design or even in other projects where the same derived component is used.
- Formal basis: data should be available to produce mathematical proofs and traceability. Because the failure mode model of a system is a hierarchy of functional groups and derived components, system level failure modes are traceable back down the fault tree to component level failure modes. This allows cut sets [6][Ch.1p3] to be determined by traversing the DAG from top level events down to their causes.
- Multiple failure modes (conjunction - where more that one failure mode is active) may be modelled from the base component level up. By breaking the problem of failure mode analysis into small stages and

building a hierarchy, the problems associated with needing to analyze all possible combinations of base level components within a system are reduced.

This is because the multiple failure modes considered within functional groups have fewer failure modes to consider at each FMMD stage. Where appropriate, multiple simultaneous failures can be modelled by introducing fault scenarios where the conjunction of failure modes is considered.

Table 3: Features of static Failure Mode analysis methodologies

Des. Crit.	FTA	FMEA	FMECA	FDEMA	FMMD
C1:	partial				✓
C2:		✓	✓	✓	✓
C3:					✓
C4:				partial	✓
C5:	partial	partial	partial	partial	✓
C6:	✓			partial	✓

5 Conclusion

Failure Mode Modular De-Composition (FMMD) is designed to be a more rigorous and 'data complete' model than the current four approaches. That is, from an FMMD model, we should be able to derive outline models that the other four methodologies would have been able to create. As this approach is modular, many of the results of analysed components may be re-used in other projects, so test efficiency is improved.

FMMD is based on generic failure modes, so it is not constrained to a particular field. It can be applied to mechanical, electrical or software domains. It can therefore be used to analyse systems comprised of electrical, mechanical and software elements in one integrated model. Furthermore the reasoning path is traceable. By being able to trace a top level event down through derived components, to base component failure modes, with each step annotated as fault scenarios, the model is easier to maintain.

The example used here is deliberately small for the purpose of being presented in a six page paper. FMMD has been applied to larger systems encompassing mechanical, electrical and software elements. FMMD represents a new technique in that it can address all the criteria in table 3, whereas the other methodologies can only cover some.

Future work

- To provide bounds on the size of the state space for the application of the methodology to certain classes of systems.
- To build a derived components library of common electrical, mechanical and software models (i.e. a collection of worked example derived components).
- To provide formal generic translations from the constructed model of any given system to the other models.

References

[1] Federal Aviation Administration. *System Safety Handbook*. http://www.faa.gov/library/ manuals/aviation /risk_management/ss_handbook/, 2008.

[2] Reliability Analysis Center. Failure mode/mechanisms distributions 1991. *United States Department of Commerce*, 1991.

[3] United States DOD. *Reliability Prediction of Electronic Equipment*. DOD, 1991.

[4] Robin E McDermot et all. *The Basics of FMEA ISBN: 0-527-76320-9*. Productivity, 1996.

[5] Nancy Leveson. *Safeware: System safety and Computers ISBN: 0-201-11972-2*. Addison-Wesley, 2005.

[6] NASA. Fault tree handbook with aerospace applications. *NASA Handbook*, 2002.

[7] Winfield Hill Paul Horowitz. *The Art of Electronics*. Cambridge, 1989.

[8] US Nuclear reg commission. Fault tree handbook. *Nuclear Safety Analysis Handbook*, 1981.

[9] E N Standard. En61508:2002 functional safety of electrical/electronic/programmable electronic safety related systems. British standards Institution http://www.bsigroup.com/, 2002.

[10] E N Standard. En298:2003 gas burner controllers with forced draft. British standards Institution http://www.bsigroup.com/, 2003.

[11] Neil Storey. *Safety-Critical Computer Systems ISBN 0-201-42787-7*. Prentice Hall, 1996.