FMEA

FMEA

This talk introduces Failure Mode Effects Analysis, and the different ways it is applied. These techniques are discussed, and then a refinement is proposed, which is essentially a modularisation of the FMEA process.

FMEA

This talk introduces Failure Mode Effects Analysis, and the different ways it is applied. These techniques are discussed, and then a refinement is proposed, which is essentially a modularisation of the FMEA process.

- Failure

FMEA

This talk introduces Failure Mode Effects Analysis, and the different ways it is applied. These techniques are discussed, and then a refinement is proposed, which is essentially a modularisation of the FMEA process.

- Failure
- Mode

FMEA

This talk introduces Failure Mode Effects Analysis, and the different ways it is applied. These techniques are discussed, and then a refinement is proposed, which is essentially a modularisation of the FMEA process.

- Failure
- Mode
- Effects

FMEA

This talk introduces Failure Mode Effects Analysis, and the different ways it is applied. These techniques are discussed, and then a refinement is proposed, which is essentially a modularisation of the FMEA process.

- Failure
- Mode
- Effects
- Analysis

- **F - Failures of given component** Consider a component in a system

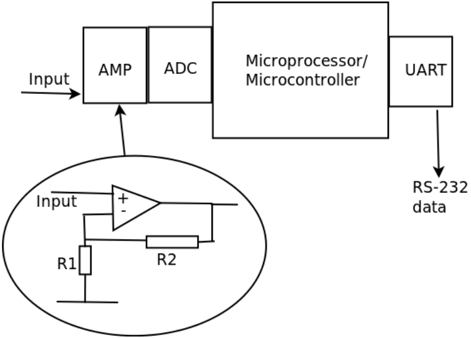
- **F - Failures of given component** Consider a component in a system
- **M - Failure Mode** Look at one of the ways in which it can fail (i.e. determine a component 'failure mode')

- **F - Failures of given component** Consider a component in a system
- **M - Failure Mode** Look at one of the ways in which it can fail (i.e. determine a component 'failure mode')
- **E - Effects** Determine the effects this failure mode will cause to the system we are examining

- **F - Failures of given component** Consider a component in a system
- **M - Failure Mode** Look at one of the ways in which it can fail (i.e. determine a component 'failure mode')
- **E - Effects** Determine the effects this failure mode will cause to the system we are examining
- **A - Analysis** Analyse how much impact this symptom will have on the environment/people/the system itsself

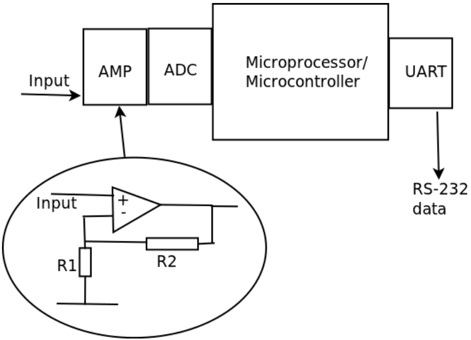
FMEA Example: Milli-volt reader

Example: Let us consider a system, in this case a milli-volt reader, consisting of instrumentation amplifiers connected to a micro-processor that reports its readings via RS-232.

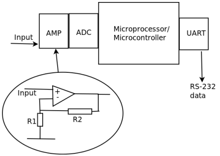


FMEA Example: Milli-volt reader

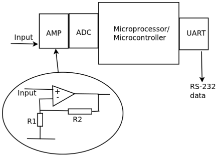
Let us perform an FMEA and consider how one of its resistors failing could affect it. For the sake of example let us choose resistor R1 in the OP-AMP gain circuitry.



FMEA Example: Milli-volt reader

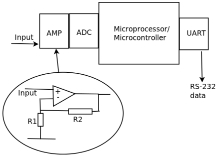


FMEA Example: Milli-volt reader



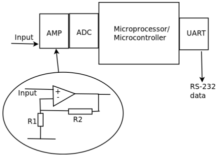
- **F - Failures of given component** The resistor (R1) could fail by going OPEN or SHORT (EN298 definition).

FMEA Example: Milli-volt reader



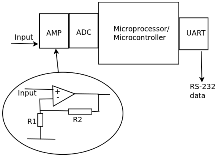
- **F - Failures of given component** The resistor (R1) could fail by going OPEN or SHORT (EN298 definition).
- **M - Failure Mode** Consider the component failure mode SHORT

FMEA Example: Milli-volt reader



- **F - Failures of given component** The resistor (R1) could fail by going OPEN or SHORT (EN298 definition).
- **M - Failure Mode** Consider the component failure mode SHORT
- **E - Effects** This will drive the minus input LOW causing a HIGH OUTPUT/READING

FMEA Example: Milli-volt reader



- **F - Failures of given component** The resistor (R1) could fail by going OPEN or SHORT (EN298 definition).
- **M - Failure Mode** Consider the component failure mode SHORT
- **E - Effects** This will drive the minus input LOW causing a HIGH OUTPUT/READING
- **A - Analysis** The reading will be out of normal range, and we will have an erroneous milli-volt reading

Note here that we have had to look at the failure mode in relation to the entire circuit.

Note here that we have had to look at the failure mode in relation to the entire circuit. We have used intuition to determine the probable effect of this failure mode.

Note here that we have had to look at the failure mode in relation to the entire circuit. We have used intuition to determine the probable effect of this failure mode. We have not examined this failure mode against every other component in the system.

Note here that we have had to look at the failure mode in relation to the entire circuit. We have used intuition to determine the probable effect of this failure mode. We have not examined this failure mode against every other component in the system. Perhaps we should.... this would be a more rigorous and complete approach in looking for system failures.

Rigorous Single Failure FMEA

Consider the analysis where we look at all the failure modes in a system, and then see how they can affect all other components within it.

Rigorous Single Failure FMEA

We need to look at a large number of failure scenarios to do this completely (all failure modes against all components). This is represented in the equation below. where N is the total number of components in the system, and f is the number of failure modes per component.

$$N.(N-1).f \tag{1}$$

Rigorous Single Failure FMEA

This would mean an order of N^2 number of checks to perform to undertake a 'rigorous FMEA'. Even small systems have typically 100 components, and they typically have 3 or more failure modes each. $100 * 99 * 3 = 29,700$.

Rigorous Double Failure FMEA

For looking at potential double failure scenarios (two components failing within a given time frame) and the order becomes N^3.

Rigorous Double Failure FMEA

For looking at potential double failure scenarios (two components failing within a given time frame) and the order becomes N^3.

$$N.(N-1).(N-2).f \tag{2}$$

Rigorous Double Failure FMEA

For looking at potential double failure scenarios (two components failing within a given time frame) and the order becomes N^3.

$$N.(N-1).(N-2).f \tag{2}$$

$100 * 99 * 98 * 3 = 2,910,600.$

Rigorous Double Failure FMEA

For looking at potential double failure scenarios (two components failing within a given time frame) and the order becomes N^3.

$$N.(N-1).(N-2).f \tag{2}$$

$100 * 99 * 98 * 3 = 2,910,600.$

.

The European Gas burner standard (EN298:2003), demands the checking of double failure scenarios (for burner lock-out scenarios).

Four main Variants of FMEA

Four main Variants of FMEA

- **PFMEA - Production**

Four main Variants of FMEA

- **PFMEA - Production** Car Manufacture etc

Four main Variants of FMEA

- **PFMEA - Production** Car Manufacture etc
- **FMECA - Criticallity**

Four main Variants of FMEA

- **PFMEA - Production** Car Manufacture etc
- **FMECA - Criticallity** Military/Space

Four main Variants of FMEA

- **PFMEA - Production** Car Manufacture etc
- **FMECA - Criticallity** Military/Space
- **FMEDA - Statistical safety**

Four main Variants of FMEA

- **PFMEA - Production** Car Manufacture etc
- **FMECA - Criticallity** Military/Space
- **FMEDA - Statistical safety** EN61508/IOC1508

Four main Variants of FMEA

- **PFMEA - Production** Car Manufacture etc
- **FMECA - Criticallity** Military/Space
- **FMEDA - Statistical safety** EN61508/IOC1508 Safety Integrity Levels

Four main Variants of FMEA

- **PFMEA - Production** Car Manufacture etc
- **FMECA - Criticallity** Military/Space
- **FMEDA - Statistical safety** EN61508/IOC1508 Safety Integrity Levels
- **DFMEA - Design or static/theoretical**

Four main Variants of FMEA

- **PFMEA - Production** Car Manufacture etc
- **FMECA - Criticallity** Military/Space
- **FMEDA - Statistical safety** EN61508/IOC1508 Safety Integrity Levels
- **DFMEA - Design or static/theoretical** EN298/EN230/UL1998

PFMEA

Production FMEA (or PFMEA), is FMEA used to prioritise, in terms of cost, problems to be addressed in product production.

PFMEA

Production FMEA (or PFMEA), is FMEA used to prioritise, in terms of cost, problems to be addressed in product production.
It focuses on known problems, determines the frequency they occur and their cost to fix.

PFMEA

Production FMEA (or PFMEA), is FMEA used to prioritise, in terms of cost, problems to be addressed in product production.
It focuses on known problems, determines the frequency they occur and their cost to fix. This is multiplied together and called an RPN number.

PFMEA

Production FMEA (or PFMEA), is FMEA used to prioritise, in terms of cost, problems to be addressed in product production. It focuses on known problems, determines the frequency they occur and their cost to fix.This is multiplied together and called an RPN number.Fixing problems with the highest RPN number will return most cost benefit.

PFMEA

Production FMEA (or PFMEA), is FMEA used to prioritise, in terms of cost, problems to be addressed in product production. It focuses on known problems, determines the frequency they occur and their cost to fix.This is multiplied together and called an RPN number.Fixing problems with the highest RPN number will return most cost benefit.

PFMEA Example

Table: FMEA Calculations

Failure Mode	P	Cost	Symptom	RPN
relay 1 n/c	$1 * 10^{-5}$	38.0	indicators fail	0.00038
relay 2 n/c	$1 * 10^{-5}$	98.0	doorlocks fail	0.00098

PFMEA Example: Ford Pinto: 1975

PFMEA Example: Ford Pinto: 1975

Figure: Burnt Out Pinto

PFMEA Example: Ford Pinto: 1975

Table: FMEA Calculations

Failure Mode	**P**	**Cost**	**Symptom**	**RPN**
relay 1 n/c	$1 * 10^{-5}$	38.0	indicators fail	0.00038
relay 2 n/c	$1 * 10^{-5}$	98.0	doorlocks fail	0.00098
rear end crash ruptured f.tank	$14.4 * 10^{-6}$	267,700	fatal fire allow	3.855
rear end crash ruptured f.tank	1	11	recall fix tank	11.0

http://www.youtube.com/watch?v=rcNeorjXMrE

FMECA - Failure Modes Effects and Criticallity Analysis

Figure: A10 Thunderbolt

Emphasis on determining criticality of failure. Applies some Bayesian statistics (probabilities of component failures and those thereby causing given system level failures).

FMECA - Failure Modes Effects and Criticality Analysis

Very similar to PFMEA, but instead of cost, a criticality or seriousness factor is ascribed to putative top level incidents.

FMECA - Failure Modes Effects and Criticality Analysis

Very similar to PFMEA, but instead of cost, a criticality or seriousness factor is ascribed to putative top level incidents.FMECA has three probability factors for component failures.

FMECA - Failure Modes Effects and Criticality Analysis

Very similar to PFMEA, but instead of cost, a criticality or seriousness factor is ascribed to putative top level incidents.FMECA has three probability factors for component failures.
FMECA λ_p value. This is the overall failure rate of a base component. This will typically be the failure rate per million (10^6) or billion (10^9) hours of operation.

FMECA - Failure Modes Effects and Criticality Analysis

Very similar to PFMEA, but instead of cost, a criticality or seriousness factor is ascribed to putative top level incidents.FMECA has three probability factors for component failures.

FMECA λ_p value. This is the overall failure rate of a base component. This will typically be the failure rate per million (10^6) or billion (10^9) hours of operation.reference MIL1991.

FMECA - Failure Modes Effects and Criticality Analysis

Very similar to PFMEA, but instead of cost, a criticality or seriousness factor is ascribed to putative top level incidents.FMECA has three probability factors for component failures.
FMECA λ_p value. This is the overall failure rate of a base component. This will typically be the failure rate per million (10^6) or billion (10^9) hours of operation.reference MIL1991.
FMECA α value. The failure mode probability, usually denoted by α is the probability of a particular failure mode occurring within a component.

FMECA - Failure Modes Effects and Criticality Analysis

Very similar to PFMEA, but instead of cost, a criticality or seriousness factor is ascribed to putative top level incidents.FMECA has three probability factors for component failures.
FMECA λ_p value. This is the overall failure rate of a base component. This will typically be the failure rate per million (10^6) or billion (10^9) hours of operation.reference MIL1991.
FMECA α value. The failure mode probability, usually denoted by α is the probability of a particular failure mode occurring within a component. reference FMD-91.

FMECA - Failure Modes Effects and Criticality Analysis

FMECA β value. The second probability factor β, is the probability that the failure mode will cause a given system failure.

FMECA - Failure Modes Effects and Criticality Analysis

FMECA β value. The second probability factor β, is the probability that the failure mode will cause a given system failure.This corresponds to 'Bayesian' probability, given a particular component failure mode, the probability of a given system level failure.

FMECA - Failure Modes Effects and Criticality Analysis

FMECA β value. The second probability factor β, is the probability that the failure mode will cause a given system failure.This corresponds to 'Bayesian' probability, given a particular component failure mode, the probability of a given system level failure. **FMECA 't' Value**

FMECA - Failure Modes Effects and Criticality Analysis

FMECA β value. The second probability factor β, is the probability that the failure mode will cause a given system failure.This corresponds to 'Bayesian' probability, given a particular component failure mode, the probability of a given system level failure. **FMECA 't' Value**The time that a system will be operating for, or the working life time of the product is represented by the variable t.

FMECA - Failure Modes Effects and Criticality Analysis

FMECA β value. The second probability factor β, is the probability that the failure mode will cause a given system failure.This corresponds to 'Bayesian' probability, given a particular component failure mode, the probability of a given system level failure. **FMECA 't' Value**The time that a system will be operating for, or the working life time of the product is represented by the variable t. **Severity 's' value** A weighting factor to indicate the seriousness of the putative system level error.

FMECA - Failure Modes Effects and Criticality Analysis

FMECA β value. The second probability factor β, is the probability that the failure mode will cause a given system failure.This corresponds to 'Bayesian' probability, given a particular component failure mode, the probability of a given system level failure. **FMECA 't' Value**The time that a system will be operating for, or the working life time of the product is represented by the variable t. **Severity 's' value** A weighting factor to indicate the seriousness of the putative system level error.

$$C_m = \beta.\alpha.\lambda_p.t.s \tag{3}$$

FMECA - Failure Modes Effects and Criticality Analysis

FMECA β value. The second probability factor β, is the probability that the failure mode will cause a given system failure.This corresponds to 'Bayesian' probability, given a particular component failure mode, the probability of a given system level failure. **FMECA 't' Value**The time that a system will be operating for, or the working life time of the product is represented by the variable t. **Severity 's' value** A weighting factor to indicate the seriousness of the putative system level error.

$$C_m = \beta.\alpha.\lambda_p.t.s \tag{3}$$

Highest C_m values would be at the top of a 'to do' list for a project manager.

FMEDA - Failure Modes Effects and Diagnostic Analysis

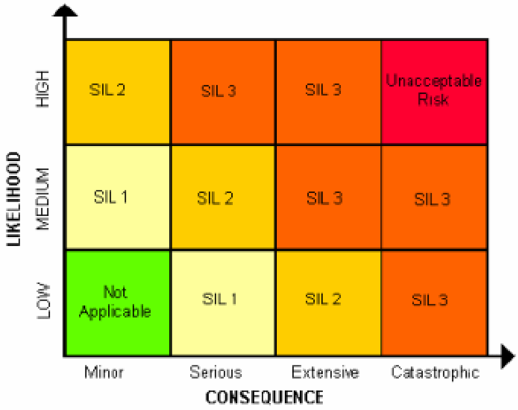


Figure: SIL requirements

FMEDA - Failure Modes Effects and Diagnostic Analysis

FMEDA - Failure Modes Effects and Diagnostic Analysis

- **Statistical Safety**

FMEDA - Failure Modes Effects and Diagnostic Analysis

- **Statistical Safety** Safety Integrity Level (SIL) standards (EN61508/IOC5108).

FMEDA - Failure Modes Effects and Diagnostic Analysis

- **Statistical Safety** Safety Integrity Level (SIL) standards (EN61508/IOC5108).
- **Diagnostics**

FMEDA - Failure Modes Effects and Diagnostic Analysis

- **Statistical Safety** Safety Integrity Level (SIL) standards (EN61508/IOC5108).
- **Diagnostics** Diagnostic or self checking elements modelled

FMEDA - Failure Modes Effects and Diagnostic Analysis

- **Statistical Safety** Safety Integrity Level (SIL) standards (EN61508/IOC5108).
- **Diagnostics** Diagnostic or self checking elements modelled
- **Complete Failure Mode Coverage**

FMEDA - Failure Modes Effects and Diagnostic Analysis

- **Statistical Safety** Safety Integrity Level (SIL) standards (EN61508/IOC5108).
- **Diagnostics** Diagnostic or self checking elements modelled
- **Complete Failure Mode Coverage** All failure modes of all components must be in the model

FMEDA - Failure Modes Effects and Diagnostic Analysis

- **Statistical Safety** Safety Integrity Level (SIL) standards (EN61508/IOC5108).
- **Diagnostics** Diagnostic or self checking elements modelled
- **Complete Failure Mode Coverage** All failure modes of all components must be in the model
- **Guidelines**

FMEDA - Failure Modes Effects and Diagnostic Analysis

- **Statistical Safety** Safety Integrity Level (SIL) standards (EN61508/IOC5108).
- **Diagnostics** Diagnostic or self checking elements modelled
- **Complete Failure Mode Coverage** All failure modes of all components must be in the model
- **Guidelines** To system architectures and development processes

FMEDA - Failure Modes Effects and Diagnostic Analysis

Failure Mode Classifications in FMEDA.

FMEDA - Failure Modes Effects and Diagnostic Analysis

Failure Mode Classifications in FMEDA.

- **Safe or Dangerous**

FMEDA - Failure Modes Effects and Diagnostic Analysis

Failure Mode Classifications in FMEDA.

- **Safe or Dangerous** Failure modes are classified SAFE or DANGEROUS

FMEDA - Failure Modes Effects and Diagnostic Analysis

Failure Mode Classifications in FMEDA.

- **Safe or Dangerous** Failure modes are classified SAFE or DANGEROUS
- **Detectable failure modes**

FMEDA - Failure Modes Effects and Diagnostic Analysis

Failure Mode Classifications in FMEDA.

- **Safe or Dangerous** Failure modes are classified SAFE or DANGEROUS
- **Detectable failure modes** Failure modes are given the attribute DETECTABLE or UNDETECTABLE

FMEDA - Failure Modes Effects and Diagnostic Analysis

Failure Mode Classifications in FMEDA.

- **Safe or Dangerous** Failure modes are classified SAFE or DANGEROUS
- **Detectable failure modes** Failure modes are given the attribute DETECTABLE or UNDETECTABLE
- **Four attributes to Failure Modes**

FMEDA - Failure Modes Effects and Diagnostic Analysis

Failure Mode Classifications in FMEDA.

- **Safe or Dangerous** Failure modes are classified SAFE or DANGEROUS
- **Detectable failure modes** Failure modes are given the attribute DETECTABLE or UNDETECTABLE
- **Four attributes to Failure Modes** All failure modes may thus be Safe Detected(SD), Safe Undetected(SU), Dangerous Detected(DD), Dangerous Undetected(DU)

FMEDA - Failure Modes Effects and Diagnostic Analysis

Failure Mode Classifications in FMEDA.

- **Safe or Dangerous** Failure modes are classified SAFE or DANGEROUS
- **Detectable failure modes** Failure modes are given the attribute DETECTABLE or UNDETECTABLE
- **Four attributes to Failure Modes** All failure modes may thus be Safe Detected(SD), Safe Undetected(SU), Dangerous Detected(DD), Dangerous Undetected(DU)
- **Four statistical properties of a system**

FMEDA - Failure Modes Effects and Diagnostic Analysis

Failure Mode Classifications in FMEDA.

- **Safe or Dangerous** Failure modes are classified SAFE or DANGEROUS
- **Detectable failure modes** Failure modes are given the attribute DETECTABLE or UNDETECTABLE
- **Four attributes to Failure Modes** All failure modes may thus be Safe Detected(SD), Safe Undetected(SU), Dangerous Detected(DD), Dangerous Undetected(DU)
- **Four statistical properties of a system** $\sum \lambda_{SD}, \sum \lambda_{SU}, \sum \lambda_{DD}, \sum \lambda_{DU}$

FMEDA - Failure Modes Effects and Diagnostic Analysis

Diagnostic Coverage. The diagnostic coverage is simply the ratio of the dangerous detected probabilities against the probability of all dangerous failures, and is normally expressed as a percentage. $\Sigma\lambda_{DD}$ represents the percentage of dangerous detected base component failure modes, and $\Sigma\lambda_D$ the total number of dangerous base component failure modes.

$$DiagnosticCoverage = \Sigma\lambda_{DD}/\Sigma\lambda_D$$

FMEDA - Failure Modes Effects and Diagnostic Analysis

The **diagnostic coverage** for safe failures, where $\Sigma\lambda_{SD}$ represents the percentage of safe detected base component failure modes, and $\Sigma\lambda_S$ the total number of safe base component failure modes, is given as

$$SF = \frac{\Sigma\lambda_{SD}}{\Sigma\lambda_S}$$

FMEDA - Failure Modes Effects and Diagnostic Analysis

Safe Failure Fraction. A key concept in FMEDA is Safe Failure Fraction (SFF). This is the ratio of safe and dangerous detected failures against all safe and dangerous failure probabilities. Again this is usually expressed as a percentage.

$$SFF = (\Sigma\lambda_S + \Sigma\lambda_{DD}) / (\Sigma\lambda_S + \Sigma\lambda_D)$$

FMEDA - Failure Modes Effects and Diagnostic Analysis

Safe Failure Fraction. A key concept in FMEDA is Safe Failure Fraction (SFF). This is the ratio of safe and dangerous detected failures against all safe and dangerous failure probabilities. Again this is usually expressed as a percentage.

$$SFF = (\Sigma\lambda_S + \Sigma\lambda_{DD}) / (\Sigma\lambda_S + \Sigma\lambda_D)$$

SFF determines how proportionately fail-safe a system is, not how reliable it is !

FMEDA - Failure Modes Effects and Diagnostic Analysis

Safe Failure Fraction. A key concept in FMEDA is Safe Failure Fraction (SFF). This is the ratio of safe and dangerous detected failures against all safe and dangerous failure probabilities. Again this is usually expressed as a percentage.

$$SFF = (\Sigma\lambda_S + \Sigma\lambda_{DD}) / (\Sigma\lambda_S + \Sigma\lambda_D)$$

SFF determines how proportionately fail-safe a system is, not how reliable it is ! Weakness in this philosophy;

FMEDA - Failure Modes Effects and Diagnostic Analysis

Safe Failure Fraction. A key concept in FMEDA is Safe Failure Fraction (SFF). This is the ratio of safe and dangerous detected failures against all safe and dangerous failure probabilities. Again this is usually expressed as a percentage.

$$SFF = (\Sigma\lambda_S + \Sigma\lambda_{DD})/(\Sigma\lambda_S + \Sigma\lambda_D)$$

SFF determines how proportionately fail-safe a system is, not how reliable it is ! Weakness in this philosophy; adding extra safe failures (even unused ones) improves the SFF.

FMEDA - Failure Modes Effects and Diagnostic Analysis

To achieve SIL levels, diagnostic coverage and SFF levels are prescribed along with hardware architectures and software techniques.

FMEDA - Failure Modes Effects and Diagnostic Analysis

To achieve SIL levels, diagnostic coverage and SFF levels are prescribed along with hardware architectures and software techniques. The overall the aim of SIL is classify the safety of a system, by statistically determining how frequently it can fail dangerously.

FMEDA - Failure Modes Effects and Diagnostic Analysis

Table: FMEA Calculations

SIL	**Low Demand** Prob of failing on demand	**Continuous Demand** Prob of failure per hour
4	10^{-5} to $< 10^{-4}$	10^{-9} to $< 10^{-8}$
3	10^{-4} to $< 10^{-3}$	10^{-8} to $< 10^{-7}$
2	10^{-3} to $< 10^{-2}$	10^{-7} to $< 10^{-6}$
1	10^{-2} to $< 10^{-1}$	10^{-6} to $< 10^{-5}$

Table adapted from EN61508-1:2001 [7.6.2.9 p33]

FMEDA - Failure Modes Effects and Diagnostic Analysis

FMEDA is a modern extension of FMEA, in that it will allow for self checking features, and provides detailed recommendations for computer/software architecture.

FMEDA - Failure Modes Effects and Diagnostic Analysis

FMEDA is a modern extension of FMEA, in that it will allow for self checking features, and provides detailed recommendations for computer/software architecture. It has a simple final result, a Safety Integrity Level (SIL) from 1 to 4 (where 4 is safest).

DESIGN FMEA: Safety Critical Approvals FMEA

Figure: FMEA Meeting

Static FMEA, Design FMEA, Approvals FMEA

DESIGN FMEA: Safety Critical Approvals FMEA

Figure: FMEA Meeting

Static FMEA, Design FMEA, Approvals FMEA
Experts from Approval House and Equipment Manufacturer discuss selected component failure modes judged to be in critical sections of the product.

DESIGN FMEA: Safety Critical Approvals FMEA

Figure: FMEA Meeting

DESIGN FMEA: Safety Critical Approvals FMEA

Figure: FMEA Meeting

- Impossible to look at all component failures let alone apply FMEA rigorously.

DESIGN FMEA: Safety Critical Approvals FMEA

Figure: FMEA Meeting

- Impossible to look at all component failures let alone apply FMEA rigorously.
- In practise, failure scenarios for critical sections are contested, and either justified or extra safety measures implemented.

DESIGN FMEA: Safety Critical Approvals FMEA

Figure: FMEA Meeting

- Impossible to look at all component failures let alone apply FMEA rigorously.
- In practise, failure scenarios for critical sections are contested, and either justified or extra safety measures implemented.
- Often Meeting notes or minutes only. Unusual for detailed arguments to be documented.

FMEA - General Criticism

FMEA - General Criticism

- FMEA type methodologies were designed for simple electro-mechanical systems of the 1940's to 1960's.

FMEA - General Criticism

- FMEA type methodologies were designed for simple electro-mechanical systems of the 1940's to 1960's.
- Reasoning Distance - component failure to system level symptom

FMEA - General Criticism

- FMEA type methodologies were designed for simple electro-mechanical systems of the 1940's to 1960's.
- Reasoning Distance - component failure to system level symptom
- State explosion - impossible to perform rigorously

FMEA - General Criticism

- FMEA type methodologies were designed for simple electro-mechanical systems of the 1940's to 1960's.
- Reasoning Distance - component failure to system level symptom
- State explosion - impossible to perform rigorously
- Difficult to re-use previous analysis work

FMEA - General Criticism

- FMEA type methodologies were designed for simple electro-mechanical systems of the 1940's to 1960's.
- Reasoning Distance - component failure to system level symptom
- State explosion - impossible to perform rigorously
- Difficult to re-use previous analysis work
- Very Difficult to model simultaneous failures.

FMEA - Better Metodology - Wish List

FMEA - Better Metodology - Wish List

- State explosion

FMEA - Better Metodology - Wish List

- State explosion
- Rigorous (total coverage)

FMEA - Better Metodology - Wish List

- State explosion
- Rigorous (total coverage)
- Reasoning Traceable

FMEA - Better Metodology - Wish List

- State explosion
- Rigorous (total coverage)
- Reasoning Traceable
- Re-useable

FMEA - Better Metodology - Wish List

- State explosion
- Rigorous (total coverage)
- Reasoning Traceable
- Re-useable
- Simultaneous failures

FMMD - Failure Mode Modular De-Composition

FMMD - Failure Mode Modular De-Composition

- Analysis occurs in small stages, within *functional groups*

FMMD - Failure Mode Modular De-Composition

- Analysis occurs in small stages, within *functional groups*
- Each *functional group* is analysed until we have a set of its symptoms of failure.

FMMD - Failure Mode Modular De-Composition

- Analysis occurs in small stages, within *functional groups*
- Each *functional group* is analysed until we have a set of its symptoms of failure.
- A *derived component* is created with its failure modes being the symptoms from the *functional group*

FMMD - Failure Mode Modular De-Composition

- Analysis occurs in small stages, within *functional groups*
- Each *functional group* is analysed until we have a set of its symptoms of failure.
- A *derived component* is created with its failure modes being the symptoms from the *functional group*
- We can now use *derived components* as higher level components

FMMD - Failure Mode Modular De-Composition

- Analysis occurs in small stages, within *functional groups*
- Each *functional group* is analysed until we have a set of its symptoms of failure.
- A *derived component* is created with its failure modes being the symptoms from the *functional group*
- We can now use *derived components* as higher level components
- We can build a failure model hierarchy in this way

FMMD - Outline of Methodology

FMMD - Outline of Methodology

- Select '*functional groups*' of components (groups that perform a well defined function).

FMMD - Outline of Methodology

- Select '*functional groups*' of components (groups that perform a well defined function).
- Using the failure modes of the components create failure scenarios.

FMMD - Outline of Methodology

- Select '*functional groups*' of components (groups that perform a well defined function).
- Using the failure modes of the components create failure scenarios.
- Analyse each failure scenario of the *functional group*.

FMMD - Outline of Methodology

- Select '*functional groups*' of components (groups that perform a well defined function).
- Using the failure modes of the components create failure scenarios.
- Analyse each failure scenario of the *functional group*.
- Collect Symptoms.

FMMD - Outline of Methodology

- Select '*functional groups*' of components (groups that perform a well defined function).
- Using the failure modes of the components create failure scenarios.
- Analyse each failure scenario of the *functional group*.
- Collect Symptoms.
- Create a '*derived component*', where its failure modes are the symptoms of the *functional group* from which it was derived.

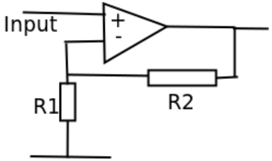
FMMD - Outline of Methodology

- Select '*functional groups*' of components (groups that perform a well defined function).
- Using the failure modes of the components create failure scenarios.
- Analyse each failure scenario of the *functional group*.
- Collect Symptoms.
- Create a '*derived component*', where its failure modes are the symptoms of the *functional group* from which it was derived.
- The *derived component* is now available to be used in higher level *functional groups*.

FMMD - Outline of Methodology

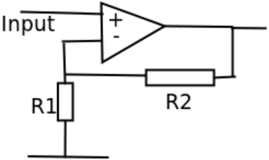
- Select '*functional groups*' of components (groups that perform a well defined function).
- Using the failure modes of the components create failure scenarios.
- Analyse each failure scenario of the *functional group*.
- Collect Symptoms.
- Create a '*derived component*', where its failure modes are the symptoms of the *functional group* from which it was derived.
- The *derived component* is now available to be used in higher level *functional groups*.
  $\bowtie (FunctionalGroup) \rightarrow DerivedComponent$

FMMD - Example - Milli Volt Amplifier



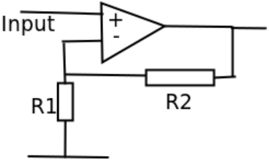
We return to the milli-volt amplifier as an example to analyse.

FMMD - Example - Milli Volt Amplifier



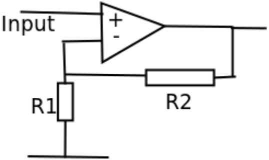
We return to the milli-volt amplifier as an example to analyse. We can begin by looking for functional groups.

FMMD - Example - Milli Volt Amplifier



We return to the milli-volt amplifier as an example to analyse. We can begin by looking for functional groups.The resistors perform a fairly common function in electronics, that of the potential divider. So our first functional group is $\{R1, R2\}$.

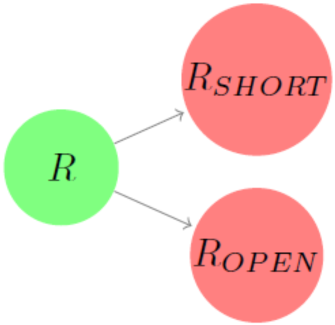
FMMD - Example - Milli Volt Amplifier



We return to the milli-volt amplifier as an example to analyse. We can begin by looking for functional groups.The resistors perform a fairly common function in electronics, that of the potential divider. So our first functional group is $\{R1, R2\}$.We can now take the failure modes for the resistors (OPEN and SHORT EN298) and see what effect each of these failures will have on the *functional group* (the potential divider).

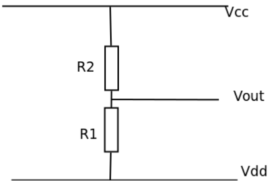
FMMD - Example - Resistor and failure modes

Resistor and its failure modes represented as a directed graph.

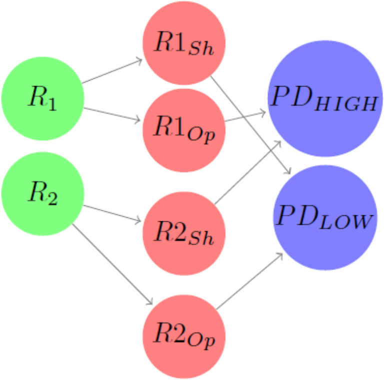


FMMD - Example - Failure mode analysis of Potential Divider

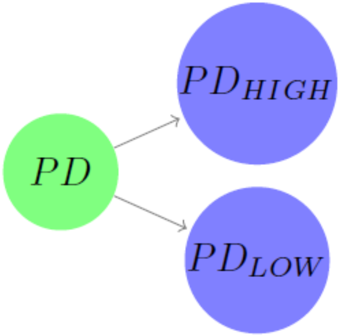
Failure Scenario / test case	**Pot Div Effect**	**Symptom**
FS1: R1 SHORT	*LOW*	*PDLow*
FS2: R1 OPEN	*HIGH*	*PDHigh*
FS3: R2 SHORT	*HIGH*	*PDHigh*
FS4: R2 OPEN	*LOW*	*PDLow*



FMMD - Example - Potential Divider as Derived Component

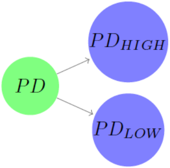


FMMD - Example - Potential Divider as Derived Component

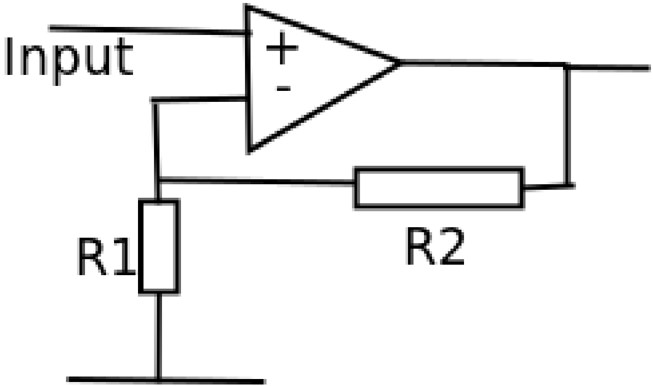


FMMD - Example - Potential Divider as Derived Component

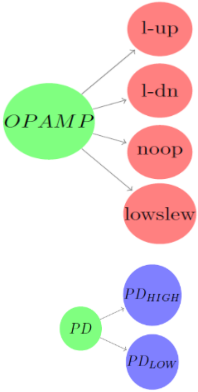
We can now use this pre-analysed potential divider 'derived component' in a higher level design.



FMMD - Example - Non Inverting OP-AMP

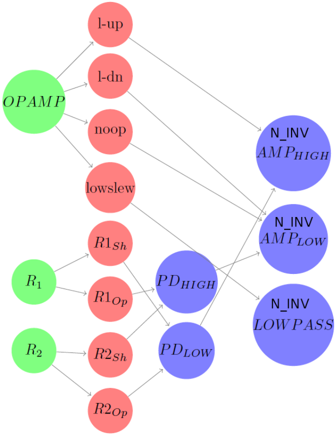


FMMD - Example - Non Inverting OP-AMP

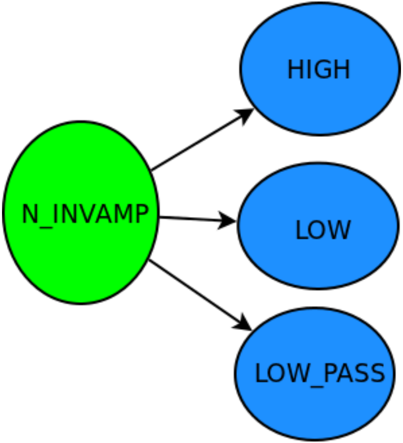


Failure Scenario	Circuit Effect	Symptom
l-up	Output High	N_INVAMP High
l-dn	Output Low	N_INVAMP Low
noop	Output Low	N_INVAMP Low
Low slew	Sluggish reactions	N_INV_LPASS
PD HIGH	Output Low	N_INVAMP Low
PD LOW	Output High	N_INVAMP High

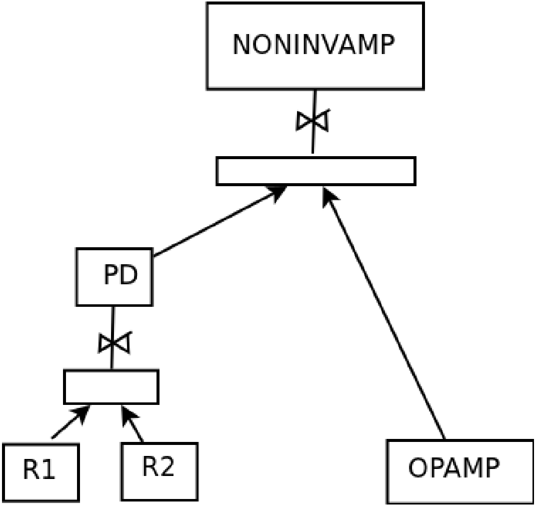
FMMD - Example - Non Inverting OP-AMP



FMMD - Example - Non Inverting OP-AMP



FMMD - Example - Non Inverting OP-AMP



FMMD - Failure Mode Modular De-Composition

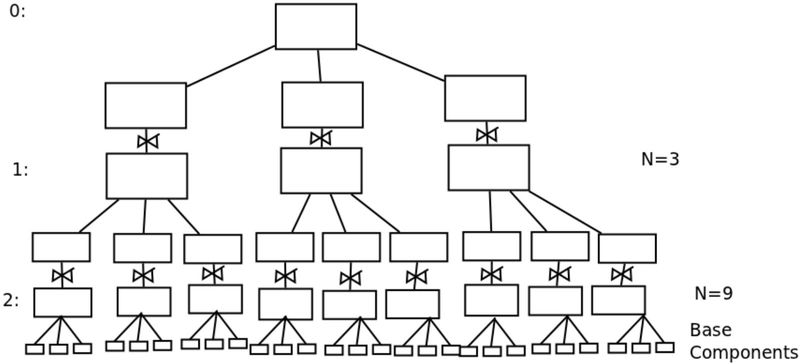


Figure: Functional Group Tree example

FMMD - Failure Mode Modular De-Composition

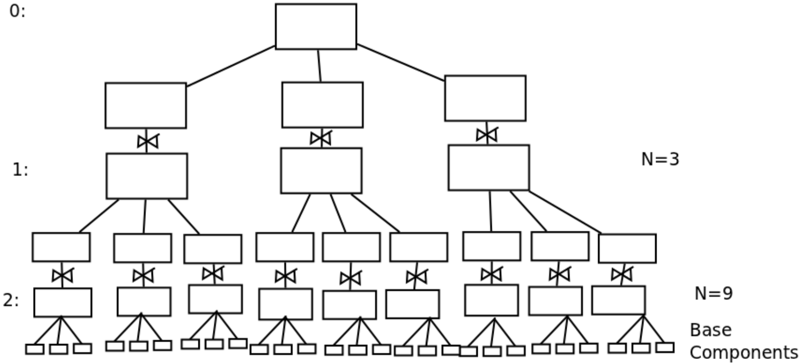


Figure: Functional Group Tree example

For the sake of example we consider each functional group to be

FMMD - Failure Mode Modular De-Composition

The fact FMMD analyses small groups of components at a time, and organises them into a hierarchy addresses the state explosion problem.

FMMD - Failure Mode Modular De-Composition

The fact FMMD analyses small groups of components at a time, and organises them into a hierarchy addresses the state explosion problem.
For FMEA where we check every component failure mode rigorously against all the other components (we could call this **RFMEA**) Where N is the number of components, we can determine the order of complexity $O(N^2)$ thus.

$$N.(N-1).f \tag{4}$$

FMMD - comparing number of checks RFMEA . . . FMMD

If we consider c to be the number of components in a *functional group*, f is the number of failure modes per component, and L to be the number of levels in the hierarchy of FMMD analysis.
We can represent the number of failure scenarios to check in an FMMD hierarchy with equation 5.

FMMD - comparing number of checks RFMEA ... FMMD

If we consider c to be the number of components in a *functional group*, f is the number of failure modes per component, and L to be the number of levels in the hierarchy of FMMD analysis.
We can represent the number of failure scenarios to check in an FMMD hierarchy with equation 5.

$$\sum_{n=0}^{L} c^n.c.f.(c-1) \qquad (5)$$

FMMD - Failure Mode Modular De-Composition

To see the effects of reducing 'state explosion' we can use an example. Let us take a system with 3 levels of FMMD analysis, with three components per functional group and three failure modes per component, and apply these formulae. Having 4 levels (in addition to the top zeroth level) will require 81 base level components.

$$81.(81-1).3 = 19440$$

$$\sum_{n=0}^{3} 3^n.3.3.(2) = 720$$

FMMD - Failure Mode Modular De-Composition

FMMD - Failure Mode Modular De-Composition

- Thus for FMMD we needed to examine 720 failure modes against functionally adjacent components, and for traditional FMEA type analysis methods, the number rises to 19440.

FMMD - Failure Mode Modular De-Composition

- Thus for FMMD we needed to examine 720 failure modes against functionally adjacent components, and for traditional FMEA type analysis methods, the number rises to 19440.
- 19440 'checks' is not practical

FMMD - Failure Mode Modular De-Composition

- Thus for FMMD we needed to examine 720 failure modes against functionally adjacent components, and for traditional FMEA type analysis methods, the number rises to 19440.
- 19440 'checks' is not practical
- 720 checks is quite alot, but...

FMMD - Failure Mode Modular De-Composition

- Thus for FMMD we needed to examine 720 failure modes against functionally adjacent components, and for traditional FMEA type analysis methods, the number rises to 19440.
- 19440 'checks' is not practical
- 720 checks is quite alot, but...
- Modules in FMMD can be re-used...

FMMD - Failure Mode Modular De-Composition

To determine all possible double simultaneous failures for rigorous FMEA the order $O(N^3)$.

$$N.(N-1).(N-2).f \tag{6}$$

Or express in terms of the level

$$c^{L+1}.(c^{L+1}-1).(c^{L+1}-2).f \tag{7}$$

FMMD - Failure Mode Modular De-Composition

To determine all possible double simultaneous failures for rigorous FMEA the order $O(N^3)$.

$$N.(N-1).(N-2).f \tag{6}$$

Or express in terms of the level

$$c^{L+1}.(c^{L+1}-1).(c^{L+1}-2).f \tag{7}$$

The FMMD case (equation 8), is cubic within the functional groups only, not all the components in the system.

$$\sum_{n=0}^{L} c^n.c.f.(c-1).(c-2) \tag{8}$$

FMMD - Failure Mode Modular De-Composition

Traceability Because each reasoning stage contains associations ($FailureMode \rightarrow Symptom$) we can trace the 'reasoning' from base level component failure mode to top level/system failure, by traversing the tree/hierarchy. This is in effect providing a 'framework' of the reasoning.

FMMD - Failure Mode Modular De-Composition

Re-usability Electronic Systems use commonly re-used functional groups (such as potential dividers, amplifier configurations etc) Once a derived component is determined, it can generally be used in other projects.

FMMD - Failure Mode Modular De-Composition

Total coverage With FMMD we can ensure that all component failure modes have been represented as a symptom in the derived components created from them. We can thus apply automated checking to ensure that no failure modes, from base or derived components have been missed in an analysis.

FMMD - Failure Mode Modular De-Composition

Conclusion: FMMD

FMMD - Failure Mode Modular De-Composition

Conclusion: FMMD

- Addresses State Explosion

FMMD - Failure Mode Modular De-Composition

Conclusion: FMMD

- Addresses State Explosion
- Addresses total coverage of all components and their failure modes

FMMD - Failure Mode Modular De-Composition

Conclusion: FMMD

- Addresses State Explosion
- Addresses total coverage of all components and their failure modes
- Provides traceable reasoning

FMMD - Failure Mode Modular De-Composition

Conclusion: FMMD

- Addresses State Explosion
- Addresses total coverage of all components and their failure modes
- Provides traceable reasoning
- derived components are re-use-able

FMMD - Failure Mode Modular De-Composition

Questions?