MISSION READY SOFTWARE
SOFTREL LLC

sales@softrel.com
321-514-4659
http://missionreadysoftware.com

Software Failure Modes Effects Analysis Services

- Our founder wrote the book on effective and efficient software failure modes effects analysis.
- Mission Ready Software has been conducting software FMEAs since the 1980s on mission and safety critical software.
- We invented the Common Defect Enumeration currently published on the DAU R&M CoP website.
- Other software FMEA analysts make the mistake of analyzing software as a black box. That approach just doesn't add value. We analyze the software from a functional viewpoint – that has been proven to work well.
- Our team of trained analysts know what works and what doesn't with regards to getting the most value from this analysis with the least amount of resources.
- We have analyzed hundreds of thousands of software failure reports and has categorized the failure modes and root causes by probability and relevance to certain application types.

The below SFMEA process complies with SAE ARP 5580 Recommended Failure Modes and Effects Analysis (FMEA) Practices for Non-Automobile Applications, IEEE 1633 Recommended Practices for Software Reliability, 2016. This SFMEA process is also employed in NASA's "Software Failure Modes Effects Criticality Analysis (SFMECA) and Software Fault Tree Analysis (SFTA)" STEP online training.

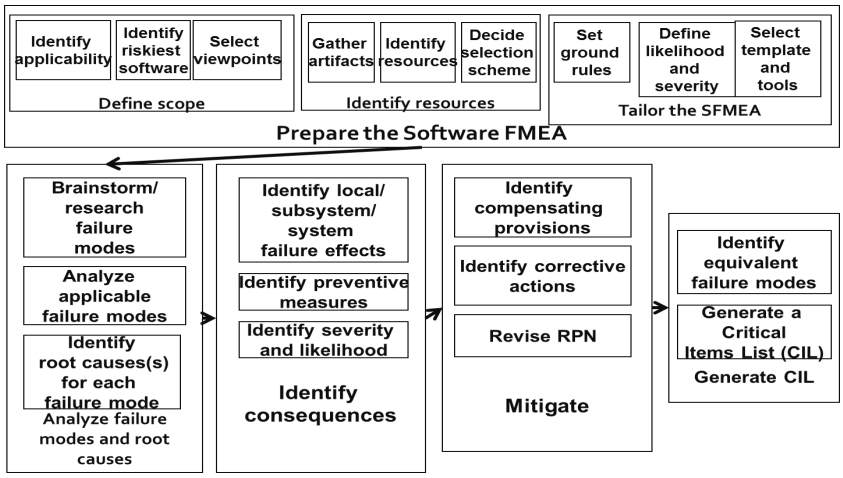

Figure 1 Software FMEA Process

Statement of work

The below is a typical statement of work which will be tailored to your application, the current state of the software (in requirements, design, code, test, etc.), time and resource limitations.

sales@softrel.com
321-514-4659
http://missionreadysoftware.com

Plan the SFMEA

The below factors determine how the SFMEA is applied to a software system under analysis. Each of these will be considered when constructing the SFMEA.

- The software product can be viewed from several viewpoints – top level, capability level, requirements level and interface level. Each of these can introduce defects that cause failures. Those defects are itemized in the Common Defect Enumeration.
- Every software application has a unique set of risks which must drive the tailoring of the viewpoints and the failure mode selection. Of the 400+ failure mode/root cause pairs that apply to nearly all software systems, typically only a few dozen are likely for a particular software system. Software FMEAs are most effective when a root cause analysis is performed up front to identify the most common failure modes and root causes.
- Every software FMEA has a unique set of goals. Those goals determine which viewpoints to select and what the finished SFMEA will be used for. Typical goals are to strengthen the requirements and test plans.
- Today's software systems are too large to analyze completely – intelligent risk based tailoring of the requirements, design and code is necessary. The requirements, design and code with the most risk is analyzed first.

Select the most relevant SFMEA viewpoints

The below Table 2 discusses when the viewpoints are relevant and the failure modes typically associated with that viewpoint. Before developing the SFMEA, it will be determined which viewpoint(s) to analyze.

Table 2 – Software FMEA viewpoints and typical failure modes

SFMEA viewpoint	When this viewpoint is relevant	Software artifacts	Typical failure modes
Functional	Any new system or any time there is a new or updated set of requirements.	• Software Requirements Specfication (SRS) • Systems Requirements Specification (SyRS) • Use Cases	• Faulty functionality - Faulty, contradictory or missing requirements for both the nominal conditions. Software does not behave as per the state requirement, performs the wrong function, performs the function when not commanded, fails to perform a function when commanded. • Faulty sequences - the right function executing in the wrong state or in the wrong order. • Faulty state management – Prohibited transitions are allowed, dead states, orphan states. • Faulty timing – The right function executing too early or too late. The function takes too long to execute. • Faulty data – Conflicting, incorrect or mismatched data requirements • Faulty error handling – Missing requirements for error handling, missing alternative paths in use cases, wrong error responses, false alarm (detects and error when there is none), detects a failure but doesn't recovery properly

sales@softrel.com
321-514-4659
http://missionreadysoftware.com

SFMEA viewpoint	When this viewpoint is relevant	Software artifacts	Typical failure modes
Interface	Anytime there is complex hardware and software interfaces or software to software interfaces. Software developers aren't co-located or working for same organization.	Interface Design documentation	Failures that happen when software communicates with other software, hardware, COTS, FOSS, OS, etc. Faulty data - Faulty interface data, conflicting units of measure (metric/english conversion) or scale (ms/seconds), faulty default values, faulty size definition, etc. Faulty error handling – Failure to detect failures in software or hardware prior to communicating

Risk based tailoring

Every software application has a unique set of risks. The below risks are what determine the selected viewpoint(s) and selected failure mode/root cause pairs. Each of these risks will be analyzed as part of the root cause analysis task.

Table 3– How risks determine the viewpoints and failure mode/root cause selection

Risk	How it effects the SFMEA
The age of the software (brand new versus very old) and whether the software is suffering from old age due to years of modifications	"Version 1" is prone to requirements related defects and poor performance. Very old software is prone to maintenance related defects.
The personnel developing the software – where are they located, how many different organizations, their experience with the software, their ability to develop the software	Weaknesses in development technique often translate to failure modes. Example – if an organization is weak at design they tend to have design related defects.
Whether the software is "stateful"	If the software is stateful then there is usually state related defects, otherwise, not
Whether the software has specific timing requirements	If the software has specific timing requirements (such as missiles and space craft) then timing related defects must be considered.
Whether there are many interfaces among components developed by different organizations	If there are multiple software organizations developing the CSCIs, the interfaces between their code is a bigger risk than otherwise, particularly if the organizations are in different physical locations
Whether the software has an extensive user interface and whether the user can cause a software failure	Usability issues have been related to several catastrophic failures within the Army and across every industry.
Whether the software will be mass deployed	If the software will be mass deployed the focus is on the "one" defect that could cause all installed sites to go down.

sales@softrel.com
321-514-4659
http://missionreadysoftware.com

Identify the specific goals of the software FMEA.

The overall direction of the SFMEA depends on the goals which can include any of the below. The goals will be updated as needed as a result of the defect root cause analysis.

Table 4 – Goals of the SFMEA

These are typical goals for SFMEA
To provide for fault tolerance in areas of high risk
To ensure that the failure modes are explicitly covered in the test plan, simulator and BIT
To strengthen the requirements to include off nominal paths and states
To strengthen the use cases to address off nominal cases
To identify failure modes that are difficult to detect in testing
To ensure that the software is user friendly
To identify information appropriate for a service or user manual (i.e. common workarounds, etc.)
To strengthen the interface design
To strengthen the detailed design (algorithms, logic, data)
To identify items applicable for a health monitoring software (HMS)

Execute the Functional FMEA (if this viewpoint is selected)

The software functional FMEA is performed on the software requirements and/or software features. The functional FMEA can and will be tailored to the requirements and failure modes that effect performance, safety or reliability. Each software requirement or feature will be analyzed one at a time against the following software failure modes:

- Faulty functionality
- Faulty sequencing
- Faulty state management
- Faulty timing
- Faulty error handling
- Faulty data definition and handling
- Faulty processing
- Faulty algorithms
- Faulty machine learning
- Faulty UI

The failure mode and root cause analysis section of the SFMEA is the core part of the FMEA. It is based entirely from the software requirements statements which must be provided by your organization. Our assessors will complete the failure mode analysis section and make an initial assessment as to the effects, severity and likelihood. Then your assessor will meet with at least one subject matter expert form your organization who will confirm the effects, severity and likelihood. The mitigation section will

sales@softrel.com
321-514-4659
http://missionreadysoftware.com

contain appropriate recommendations for changing the requirements or use cases, and developing tests.

Execute the Interface FMEA (if selected)

The software interface FMEA is performed on the interface design specification. The interface FMEA can and will be tailored to the interfaces and failure modes that effect performance, safety or reliability. Each interface will be analyzed one at a time against the following software failure modes:

- Faulty data handling
- Faulty error handling

The defect root cause analysis task will determine if the interface SFMEA is relevant. The failure mode and root cause analysis section of the interface SFMEA is the core part of the FMEA. It is based entirely from the interface design specifications. The interface design spec and must be provided by your organization. In the event that there isn't an IDS or some data is missing from the IDS - that is in itself a failure mode which can be identified on the SFMEA. Your assessor will complete the failure mode analysis section and make an initial assessment as to the effects, severity and likelihood. Then your assessor will meet with at least one subject matter expert form your organization who will confirm the effects, severity and likelihood. The mitigation section will contain appropriate recommendations for changing the interface design, and developing tests.

Related products and training

Related products	Related training
Requs AI Predict Software FMEA	Software FMEA Training

Pricing

Call 321-514-4659 for quotation.