Using FMEA to Improve Software Reliability

Kraig Strong - Tektronix
What don’t we like about (most) quality processes?
They are time consuming
They are cumbersome
They aren’t flexible
Failure Mode and Effects Analysis
Why FMEA?
• Early Identification of Failures
• Lightweight, quick, and flexible
• Well Established
• Better Planning and Scheduling
• Early Test Planning
• Single Worksheet Summary
• Requires Minimal Training
• Drop in supplement to current practices
Key Elements

• Not intended for entire system.
• Team activity with one or more meetings
• Sub-system owner, SW lead, QA, and domain expert(s) involved.
• FMEA Worksheet
• FMEA Process Steps
# FMEA Worksheet

## Failure Mode & Effect Analysis

<table>
<thead>
<tr>
<th>Component / Function</th>
<th>Potential Failure Mode</th>
<th>Effect of Potential Failure</th>
<th>Target of Potential Failure</th>
<th>Cause of Potential Failure</th>
<th>Current Controls</th>
<th>D</th>
<th>RPN</th>
<th>Recommended Actions</th>
<th>Responsibility &amp; Target Completion Date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Prevention</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Detection</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Increment 1

<table>
<thead>
<tr>
<th>D</th>
<th>RPN</th>
<th>Recommended Actions</th>
<th>Responsibility &amp; Target Completion Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Manufacturing Process FMEA
<table>
<thead>
<tr>
<th>Component / Function</th>
<th>Potential Failure Mode</th>
<th>Effect of Potential Failure</th>
<th>Target of Potential Failure</th>
<th>Cause of Potential Failure</th>
<th>Current Controls</th>
<th>D</th>
<th>RPN</th>
<th>Recommended Actions</th>
<th>Responsibility &amp; Target Completion Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Clean the sheet metal with alcohol</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Place thermal tape on border</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Clean the bottom of the heat sink with IPA</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. Place heat sink on thermal tape and apply heavy pressure</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. Clean the top of the heat sink with alcohol</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6. Place LED strip on top of the heat sink. Apply heavy pressure without placing pressure on LEDs</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
FMEA Steps

• Define Failure Modes- ‘What can go wrong here?’
• Define Effects – ‘What will happen then?’
• Describe Targets – ‘Who will suffer from failure?’
• Find Root Causes – ‘Why will that happen?’
• Prioritize the Risks – ‘What is the severity?’
• Define Solution Actions – ‘How can this be prevented?’
• Describe current Prevention and Detection methods – ‘What is currently being done?’
FMEA Steps

- Define Failure Modes - ‘What can go wrong here?’
- Define Effects – ‘What will happen then?’
- Describe Targets – ‘Who will suffer from failure?’
- Find Root Causes – ‘Why will that happen?’
- Prioritize the Risks – ‘What is the severity?’
- Define Solution Actions – ‘How can this be prevented?’
- Describe current Prevention and Detection methods – ‘What is currently being done?’
FMEA Steps

• Define Failure Modes- ‘What can go wrong here?’
• Define Effects – ‘What will happen then?’
• **Describe Targets** – ‘Who will suffer from failure?’
• Find Root Causes – ‘Why will that happen?’
• Prioritize the Risks – ‘What is the severity?’
• Define Solution Actions – ‘How can this be prevented?’
• Describe current Prevention and Detection methods – ‘What is currently being done?’
FMEA Steps

• Define Failure Modes- ‘What can go wrong here?’
• Define Effects – ‘What will happen then?’
• Describe Targets – ‘Who will suffer from failure?’
• Find Root Causes – ‘Why will that happen?’
• Prioritize the Risks – ‘What is the severity?’
• Define Solution Actions – ‘How can this be prevented?’
• Describe current Prevention and Detection methods – ‘What is currently being done?’
FMEA Steps

• Define Failure Modes- ‘What can go wrong here?’
• Define Effects – ‘What will happen then?’
• Describe Targets – ‘Who will suffer from failure?’
• Find Root Causes – ‘Why will that happen?’
• Prioritize the Risks – ‘What is the severity?’
• Define Solution Actions – ‘How can this be prevented?’
• Describe current Prevention and Detection methods – ‘What is currently being done?’
FMEA Steps

• Define Failure Modes - ‘What can go wrong here?’
• Define Effects – ‘What will happen then?’
• Describe Targets – ‘Who will suffer from failure?’
• Find Root Causes – ‘Why will that happen?’
• Prioritize the Risks – ‘What is the severity?’
• Define Solution Actions – ‘How can this be prevented?’
• Describe current Prevention and Detection methods – ‘What is currently being done?’
FMEA Steps

- Define Failure Modes- ‘What can go wrong here?’
- Define Effects – ‘What will happen then?’
- Describe Targets – ‘Who will suffer from failure?’
- Find Root Causes – ‘Why will that happen?’
- Prioritize the Risks – ‘What is the severity?’
- Define Solution Actions – ‘How can this be prevented?’
- Describe current Prevention and Detection methods – ‘What is currently being done?’
How Can This be Translated to Software?
FMEA Steps

• Define Failure Modes- ‘What can go wrong here?’
• Define Effects – ‘What will happen then?’
• Describe Targets – ‘Who will suffer from failure?’
• Find Root Causes – ‘Why will that happen?’
• Prioritize the Risks – ‘What is the severity?’
• Define Solution Actions – ‘How can this be prevented?’
• Describe current Prevention and Detection methods – ‘What is currently being done?’
Function Blocks & the Functional Block Diagram
User fills out purchasing form and clicks purchase

Gather data and verify complete and valid entries

Establish Connection

Authentication

Send encrypted data

Confirmation to client

Report success/failure to user
FMEA Steps

• Define Failure Modes- ‘What can go wrong here?’
• Define Effects – ‘What will happen then?’
• Describe Targets – ‘Who will suffer from failure?’
• Find Root Causes – ‘Why will that happen?’
• Prioritize the Risks – ‘What is the severity?’
• Define Solution Actions – ‘How can this be prevented?’
• Describe current Prevention and Detection methods – ‘What is currently being done?’
<table>
<thead>
<tr>
<th>Step #</th>
<th>Step Name</th>
<th>Failure Mode</th>
<th>Effects</th>
<th>Targets</th>
<th>Root Cause</th>
<th>S</th>
<th>O</th>
<th>D</th>
<th>RPN</th>
<th>Solution Actions</th>
<th>Current Methods</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>User fills out purchasing form and clicks purchase</td>
<td>SQL Injection appears as valid entry</td>
<td>Data theft or database corruption</td>
<td>Customers and Company</td>
<td>SQL injection not caught in verifying valid entries</td>
<td>10</td>
<td>3</td>
<td>2</td>
<td>60</td>
<td>Check for SQL injections in all fields</td>
<td>N/A</td>
</tr>
<tr>
<td>2</td>
<td>Gather data and verify complete and valid entries</td>
<td>SQL Injection appears as valid entry</td>
<td>Data theft or database corruption</td>
<td>Customers and Company</td>
<td>SQL injection not caught in verifying valid entries</td>
<td>10</td>
<td>3</td>
<td>2</td>
<td>60</td>
<td>Check for SQL injections in all fields</td>
<td>N/A</td>
</tr>
<tr>
<td>3</td>
<td>Establish connection with server</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Secure authentication with server</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Send encrypted data</td>
<td>User hits back/refresh causing data to be resent</td>
<td>multiple or incomplete orders being sent to the server</td>
<td>Customer</td>
<td>User hitting back/refresh prior to confirmation</td>
<td>7</td>
<td>5</td>
<td>1</td>
<td>35</td>
<td>Disallow multiple purchases within a specified timeframe from a specific user</td>
<td>Display a warning message to not hit back/refresh</td>
</tr>
<tr>
<td>6</td>
<td>Confirmation to client</td>
<td>Client model locked so it is not updated.</td>
<td>Incorrect status report to user</td>
<td>Customer and Company reputation</td>
<td>Semaphore placed on client model during update time</td>
<td>7</td>
<td>2</td>
<td>1</td>
<td>14</td>
<td>Have a queue to handle communication from server</td>
<td>N/A</td>
</tr>
<tr>
<td>7</td>
<td>Report success/failure to user</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
FMEA is **NOT** a Code Review
What is the Best Time for FMEA?

• Earlier the better
• Majority of requirements need to be defined
  – Solutions can be designed in HW or SW
  – Design, Requirements, and Documentation bugs
  – Jump start on test planning
  – Flush out new requirements
• Can be performed at any time, but less beneficial
Real World Results – DVM Autorange

- Clarification on wording required in SRS
- Created new test cases
- New communication channel with other subsystem required.
The Team’s Thoughts

• “It’s nice when the process doesn’t get in the way of improving quality.”
• “Well worth the 1.5 hours it took to complete.”
• “It didn’t feel like a formal process. It felt like a casual discussion amongst engineers.”
More Real World Results

• Checking for drive full, or read-only
• Out of memory (RAM).
• Dealing with loss of internet connection
Lessons Learned

• “What if?” thinking
• Additional emphasis on quality in early stages
• Flexibility to solve problems in HW or SW
• Not a catch-all
Recommendations
Common Mistakes

- Assuming all failures are caused by HW
- Attempting to cover 100%
- Not following through with solutions
- Allowing low-level conversations
- Not having appropriate experts
- Starting too late
Questions?