Comparing Failure Rates for Safety Devices

FMEDA Prediction vs OREDA Estimation
Iwan van Beurden, exida

• Vice President Product Development, Chief Technology Officer
• Supports exida’s End-user services, exida’s Manufacturer services, and exida certification activities.
• Responsible for exida end-user software, including exSILentia®, SILStat™, SILAlarm™, and CyberPHAx™
• Member ISA S84 committee
• Performs
  – IEC 61508 development support
  – Functional Safety Assessments, Audits
  – Variety of reliability analyses
  – SIL Selections
  – SIL Verifications
  – exida and ISA instructor
Contents

• Introduction
• Failure Rate Estimation
• Failure Rate Prediction
• FMEDA Prediction vs OREDA Estimation
• Conclusion
INTRODUCTION
Introduction

• Functional Safety Standards provide safety lifecycle framework for E/E/PES systems
• IEC 61511 addresses SIFs in Process Industry applications
Probabilistic Analysis

• SIF conceptual design is evaluated through probabilistic analysis
• Inputs are performance parameters including failure rates for all devices
FAILURE RATE ESTIMATION
Failure Rate Sources - Estimation

- Industry Databases
- Committee Estimates
- Manufacturer Warranty Analysis
- End User Field Failure Data Studies
Industry Databases

- Field failure data gathered from variety of sources
- Aggregated results published
- For example
  - OREDA
    - Operated by DNV, Data Analysis by SINTEF
    - Useful data on process equipment
    - Latest public release in 2015
    - Failure rates based on given population and recorded operating hours
  - OREDA Example
    - Pressure transmitter
    - Total mean failure rate 0.42E-6/hr
    - Population 32 units
Committee Estimates

- Failure rates estimated based on committee member experience
- Methods rarely published
- Data good for comparison
- For example
  - AIChE, CCPS Guideline documents
Manufacturer Warranty Analysis

• Real Data!

• Calculation methods vary widely
• Don’t know what percentage of actual failures are returned
  – Operational hours sometimes estimated based on shipping records
    while assuming that all failures are returned (very optimistic)
• Narrow definition of “Failure”
  – Many manufacturers classify returned items as a “Failure” only if a
    manufacturing defect is found
  – Many returned items are marked “No Problem Found” or “Systematic
    Failure”

• Data can be valuable to identify root causes and compare to
  establish lower bounds on failure rate
End User Field Failure Data Analysis

• Excellent source for site specific data
• Many existing data gathering systems are weak
  – Different definitions of “Failure” / not all “Failures” recorded
  – Variations of amount of data collected
  – Categorizing and Merging Technologies
  – Lack of fault isolation
• Data collection process can vary by an order of magnitude or more!
  – When is a failure report written?
  – What is the definition of failure?
  – Are "as found" conditions recorded during a proof test?
  – What were the operating conditions?
FAILURE RATE PREDICTION
Problems with Estimation

• One problem with all failure rate estimation techniques is product obsolescence
• Number of failures recorded per end-user site relatively low, i.e. statistical analysis not viable
• No information available on new product designs
Failure Rate Sources – Prediction

• B10d / HALT
  – Highly Accelerated Life Test
• FMEDA
  – Failure Modes, Effects, and Diagnostic Analysis
B10d (Cycle Test) Failure Data

• Cycle test for mechanical / electro-mechanical products
  – Test until 10% of units under test fail (B10 Point)
  – Convert number of cycles until failure to time period
  – Failure rate calculated by dividing 10% failure count by time period
  – $\lambda_D$ is assumed 50% of total failure rate, $\lambda_S$ is 50%, no other failure modes are assumed to exist

• Assumptions
  – All failures due entirely to premature wear-out
  – Application has constant dynamic operation
Failure Modes, Effects, and Diagnostic Analysis (FMEDA)

• A predictive failure rate method developed by exida engineers
• Study of each component and how the component failure will affect the product
• Estimate (or test) how well automatic diagnostics and proof test will detect the component failure
• Uses a component database that accounts for design strength versus a predefined environment
FMEDA Considers

- Component Failure Rates are a function of operating environment
  - Application
  - Operating Conditions
- Study Design Strength
- Predict Useful Life
- Predict test coverage
  - Automatic Diagnostic
  - Proof Test
FMEDA PREDICTION VS OREDA ESTIMATION
Pressure Transmitter Failure Rate Comparison

OREDA: 4.20E-07 failures/hour
DOW: 4.96E-07 failures/hour
FMEDA average: 5.02E-07 failures/hour
When comparing failure rate data, it is essential to understand the assumptions made used to derive the each data set.
Ball Valve Subsystem Failure Rate Comparison

Comparison of Equivalent Ball Valve Subsystems

Upper Confidence Limits

Lower Confidence Limits

Failure rate / 10^6 hrs

OREDA MEANS

FMEDA MAX
FMEDA MEAN
FMEDA MIN
OREDA 2015
OREDA 2009

COT- FS  COT-TSO  OOT
Gate Valve Subsystem Failure Rate Comparison

Comparison of Equivalent Gate Valve Subsystems

- FMEDA MAX
- FMEDA MEAN
- FMEDA MIN
- OREDA 2015
- OREDA 2009

Failure rate / 10^6 hrs

Upper Confidence Limits

Lower Confidence Limits
CONCLUSION
Determine Realistic Failure Rate Ranges

<table>
<thead>
<tr>
<th>Application</th>
<th>ESD Ball Valve Subsystem</th>
<th>ESD Gate Valve Subsystem</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>COT</td>
<td>TSO</td>
</tr>
<tr>
<td>FMEDA $\lambda_{D \text{ MAX}}$</td>
<td>3.95</td>
<td>5.10</td>
</tr>
<tr>
<td>ORED $\lambda_D$</td>
<td>1.91</td>
<td>1.91</td>
</tr>
<tr>
<td>FMEDA $\lambda_{D \text{ AVG}}$</td>
<td>1.45</td>
<td>2.27</td>
</tr>
<tr>
<td>FMEDA $\lambda_{D \text{ MIN}}$</td>
<td>0.69</td>
<td>1.25</td>
</tr>
</tbody>
</table>

2015 edition

Failure rates per 10^6 hours
Need for Failure Rate Prediction

- Application Specific, Product Specific, field failure data is the best source for real life failure rates
- Collecting failure rate data takes time
  - Product may become obsolete
  - Typically not enough data for statistical analysis
- No field data available for new product designs

- FMEDA Failure Rate Prediction
  - Requires clear definition of failure
  - Requires good component data handbook
  - Yields realistic failure data based on design strength analysis and expected operational stress conditions
QUESTIONS?