The Impact of Imperfect Manual Testing, Bypassing, and Bubba on Safety Instrumented System Performance

Paul Gruhn, P.E.
Rockwell Automation
Introduction of Speaker

Paul Gruhn, P.E.

- Global Process Safety Consultant at Rockwell Automation
- Safety Systems Specialist for >25 years
- ISA Fellow
- Member of ISA 84 (SIS) & 101 (HMI) committees
- Developer & Instructor for ISA’s courses on Safety Instrumented Systems (8 days of material)
- Primary author of ISA book on SIS
- Developer of 1st commercial SIS modeling software
- Licensed Professional Engineer in Texas (and member of CSE exam team)
- ISA 84 Expert
Questions...

1. How many of you assume perfect manual testing in your PFD calculations?

2. How many of you include bypassing in your PFD calculations?

3. How many of you include the impact of Bubba in your PFD calculations?

4. How much of an impact do you think it would have if you did?
Failure Modes

With a safety system, the concern shouldn’t so much be with how the system *operates*, but rather how the system *fails*.

Safety systems can fail in *two* ways:

**Safe failures**
- initiating
- overt
- spurious
- costly downtime

**Dangerous failures**
- inhibiting
- covert
- potentially dangerous
- must find by testing

\[ D \times U = \]
Detecting Dangerous Failures

• Some devices are ‘dumb’ and have no diagnostics (e.g., a pressure switch, solenoid operated valve)
  – Failures must be tested for manually

• Some devices are ‘smart’ and do have diagnostics (e.g., transmitter, PLC)
  – Failures can be detected automatically

• However, no device has perfect diagnostics, and manual testing is never perfect
PFDavg Formula for 1oo1

\[
PFD_{avg} = [\lambda_{DD} \times (MTTR + TI_A/2)] + [\lambda_{DU} \times TI_M/2] + [\lambda_{DN} \times Life/2] + [BD/TI_M]
\]

Where:

- \( TI_A \) = Automatic test interval
- \( MTTR \) = Mean Time To Repair
- \( TI_M \) = Manual test interval
- \( BD \) = Bypass Duration
- \( \lambda_{DD} \) = Dangerous detected failure rate
- \( \lambda_{DU} \) = Dangerous undetected failure rate
- \( \lambda_{DN} \) = Dangerous never detected failure rate

Note: The above formula is valid as long as \( \lambda \ll TI_M \) (or \( MTTF \gg TI_M \))

\[
\begin{align*}
\lambda_{DD} &= \lambda_D \times C_A \\
\lambda_{DU} &= \lambda_D \times (1 - C_A) \times C_M \\
\lambda_{DN} &= \lambda_D \times (1 - C_A) \times (1 - C_M) \\
\lambda_D &= \lambda_{DD} + \lambda_{DU} + \lambda_{DN}
\end{align*}
\]
Base Case Assumptions:

1. Single smart transmitter with an 80 year MTTF$_D$ ($1/\lambda_D$), 90% C$_A$
2. Fault tolerant safety PLC certified for use in SIL 3
3. Single valve with a 50 year MTTF$_D$ ($1/\lambda_D$), weekly partial stroke testing claiming 80% C$_A$
4. Yearly manual testing that is 100% effective
5. No bypassing

RRF (1/PFD) = 350
## Safety Integrity Levels

<table>
<thead>
<tr>
<th>Safety Integrity Level</th>
<th>Probability of Failure on Demand (PFD)</th>
<th>Risk Reduction Factor (1/PFD)</th>
<th>Safety Availability (1-PFD)</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>≥.00001 to &lt;.0001</td>
<td>&gt; 10,000 to ≤ 100,000</td>
<td>&gt; 99.99 to ≤ 99.999</td>
</tr>
<tr>
<td>3</td>
<td>≥.0001 to &lt;.001</td>
<td>&gt; 1,000 to ≤ 10,000</td>
<td>&gt; 99.9 to ≤ 99.99</td>
</tr>
<tr>
<td>2</td>
<td>≥.001 to &lt;.01</td>
<td>&gt; 100 to ≤ 1,000</td>
<td>&gt; 99 to ≤ 99.9</td>
</tr>
<tr>
<td>1</td>
<td>≥.01 to &lt;.1</td>
<td>&gt; 10 to ≤ 100</td>
<td>&gt; 90 to ≤ 99</td>
</tr>
</tbody>
</table>

For “Demand Mode” of operation
## Fault Tolerance Requirements

<table>
<thead>
<tr>
<th>SIL</th>
<th>Minimum Hardware Fault Tolerance</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>See IEC 61508</td>
</tr>
</tbody>
</table>

For field devices and non-PE logic solvers.

The numbers may need to be reduced or increased by one under certain circumstances. See sections 11.4.3 - 11.4.5.
Impact of Imperfect Testing

- 100% Manual Test Coverage: RRF = 350
- 95% Manual Test Coverage: RRF = 190
- 90% Manual Test Coverage: RRF = 130
- 80% Manual Test Coverage: RRF = 82
- 70% Manual Test Coverage: RRF = 59
Impact of Bypassing

- 0 hours bypass duration: 350 RRF
- 1 hour bypass duration: 340 RRF
- 1 day bypass duration: 180 RRF
- 1 week bypass duration: 45 RRF
- 1 month bypass duration: 13 RRF

1,000
100
10

Bypass Duration

71st Annual Instrumentation and Automation Symposium for the Process Industries
## Impact of Both

<table>
<thead>
<tr>
<th>Time in Bypass</th>
<th>Manual Test Coverage %</th>
<th>RRF</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>100</td>
<td>350</td>
</tr>
<tr>
<td>1 hour</td>
<td>95</td>
<td>190</td>
</tr>
<tr>
<td>1 day</td>
<td>90</td>
<td>77</td>
</tr>
<tr>
<td>1 week</td>
<td>80</td>
<td>20</td>
</tr>
<tr>
<td>1 month</td>
<td>70</td>
<td>&lt;10</td>
</tr>
</tbody>
</table>
Impact of Bubba

• How many times have you made an error doing a routine activity?
• How often have you found something installed wrong?
• How often have you found something engineered wrong?
• An error probability of .001 is optimistic
• If included, SIL 2 may be the limit of any system
Conclusions

1. Manual testing must be as thorough and complete as possible
   — Or you will not be meeting your performance target

2. Do not leave systems in bypass for longer than absolutely necessary
   — Or you will not be meeting your performance target

3. Model ‘reality’, not the ‘ideal’
   — All models are wrong, some are just less wrong than others