Practical and Robust Implementation of the IEC Functional Safety Standards
Abstract

• The release and adoption of IEC 61508 and IEC 61511 has created new requirements for all organizations involved with equipment used in safety related systems. As these functional safety standards are applied more broadly across industry and referenced more frequently as examples of best practice by industry and product standards the importance of meeting them is increasing. The requirements of the standards are new to many end users, EPCs, and manufacturers of valve, actuator, and other devices used in the final element which can result in effort invested in areas that do not guarantee compliance or increased safety reliability.

• This presentation will review the functional safety standards along with the steps necessary to meet them. IEC 61508 will be examined including the Safety Lifecycle, keys documentation necessary, and information that is supplied to end users. IEC 61511 will be reviewed to examine the impact of the information supplied by manufacturers. Examples from both the manufacturer and end user viewpoint will be provided to illustrate common pitfalls as well as best practices.
Chris O’Brien is a Partner with Exida Consulting. He has over 25 years experience in the design, manufacturing and marketing of process automation, reserve power systems, and safety related equipment. He focuses on supporting new and existing customers with their implementation of the IEC 61508 and IEC 61511 functional safety standards as well as reliability analysis for mechanical devices.

He was formerly Vice President of the Power Systems Business Unit of C&D Technologies, a business that specialized in the design and implementation of high reliability back up power systems. Prior to that, he was with Moore Products/Siemens Energy and Automation where he held several positions including General Manager of the Instrumentation Division.

Chris is the author of Final Elements and the IEC 61508 and IEC 61511 Functional Safety Standards and has been awarded 5 patents, including a patent of the industry's first safety rated pressure transmitter. He has a Bachelors of Mechanical Engineering from Villanova University.
Topics

• The Functional Safety Standards
• What are Customers Doing?
• Critical Issues
• Importance of Data Integrity
• Product Certification
• Roles and Responsibilities
The Functional Safety Standards

• What is Functional Safety?
• Scope of IEC 61508
• How the standard apply to Mechanical Devices?
• What does the standard address?
  – Safety Lifecycle
  – Systemic Faults
  – Random Faults
IEC/EN 61508 – Functional Safety

Functional Safety Goal – The automatic safety function will perform the intended function correctly or the system will fail in a predictable (safe) manner.
IEC/EN 61508 – Consensus Standard

HSE
PES
SA
S84
DIN V 1925
DINV VDE0801
EWICS

IEC61508

March 11, 2014
Copyright © exida.com LLC 2000-2014
IEC 61508 – Summary

- Applies to “Automatic Protection Systems” – E/E/PE
- Provides measures of protection against random hardware failures and “systematic” design failures
- Can be applied to PROJECT level work – bespoke (turnkey) systems
- Can be applied to PRODUCT level work – off the shelf products applied in many applications
• Targets **Suppliers**
  
  – Requirements for suppliers of process control and instrumentation for component / element or sub-system safety
  
  – End Users should seek suppliers with products certified to this standard by a reputable certifying agency
IEC 61508 Enforcement

• In some countries, the standard has been accepted by governments with the force of law
• In most situations, the standard typically is cited as best practice
  – Often required by end-user customers as part of project contracts
• When accidents happen, the standard can be cited in civil cases as a commonly accepted standard of performance
IEC/EN 61508 – E/E/PE

IEC 61508 states it was written for E/E/PE based systems.

E – electrical

E – electronic

PE – programmable electronic

Therefore not applicable for mechanical products??
Just Google It

A) Scope

A1) Is IEC 61508 relevant to me?

A2) What systems does IEC 61508 cover?

A3) Give me some practical examples

A4) How does IEC 61508 apply where E/E/PE technology makes up only a small part of the safety-related system?

IEC 61508 is applicable to any safety-related system that contains an E/E/PE device.

This applicability is appropriate because many requirements, particularly in IEC 61508-1, are not technology specific. Indeed, early development phases (such as initial concept, overall scope definition, hazard and risk analysis and specifying the overall safety requirements) may take place before the implementation technology has been decided.

Even during later phases such as realisation, specific functional safety requirements apply directly to non-E/EPE devices, such as mechanical components, as well as E/EPE devices. For example, the requirements for hardware reliability and fault tolerance in IEC 61508-2 directly relate to the properties of all components in the E/EPE safety-related system, whether or not they include E/EPE technology.

For low complexity E/E/PE safety-related systems, it is possible to comply with IEC 61508 while not meeting every requirement of the standard.
A4) How does IEC 61058 apply where E/E/PE technology makes up only a small part of the safety-related system?

IEC 61508 is applicable to any safety-related system that contains an E/E/PE device.

This applicability is appropriate because many requirements, particularly in IEC 61508-1, are not technology specific. Indeed, early development phases (such as initial concept, overall scope definition, hazard and risk analysis and specifying the overall safety requirements) may take place before the implementation technology has been decided.

Even during later phases such as realisation, specific functional safety requirements apply directly to non-E/E/PE devices, such as mechanical components, as well as E/E/PE devices. For example, the requirements for hardware reliability and fault tolerance in IEC 61508-2 directly relate to the properties of all components in the E/E/PE safety-related system, whether or not they include E/E/PE technology.

For low complexity E/E/PE safety-related systems, it is possible to comply with IEC 61508 while not meeting every requirement of the standard.
The Standards

International Performance Based Standard For All Industries (Applies to suppliers)

IEC61511 : Process Industry Sector
US uses essentially identical ISA 84.00.01-2004

IEC62061 : Machinery Sector

IEC61513 : Nuclear Sector
What are Customers Doing?

- IEC 61511
- Why is there a need?
- Safety Instrumented Systems
- Safety Instrumented Functions
- The Safety Lifecycle
IEC 61511 Standard

• Targets **End Users**, Engineering Contractors and Integrators in process industries
• Covers the entire SIS Life Cycle
  – Risk Analysis
  – Performance based design
  – Operations and Maintenance
• Performance NOT Prescriptive
• End user applications
  – Independent Functional Safety Assessments
• 3 sections
  – Requirements
  – Guidelines
  – SIL Selection
Why is There a Need?
IEC 61511 defines a Safety Instrumented System (SIS) as:

“instrumented system used to implement one or more safety instrumented functions. A SIS is composed of any combination of sensor(s), logic solver(s), and final element(s).” IEC 61511 Part 1 : 3.2.72
Practitioners often prefer a more functional definition of SIS such as:

“A SIS is defined as a system composed of sensors, logic solvers and final elements designed for the purpose of:

1. **Automatically taking an industrial process to a safe state when specified conditions are violated**;

2. **Permit a process to move forward in a safe manner when specified conditions allow (permissive functions)**;

3. **Taking action to mitigate the consequences of an industrial hazard.**”

* BPCS: Basic Process Control System
Safety Instrumented Function (SIF)

“Safety function with a specified SIL which is necessary to achieve functional safety and which can be either a safety instrumented protection function or a safety instrumented control function.”

IEC 61511 Part 1 : 3.2.71
Safety Instrumented Function Examples

- On detecting high temperature, prevent column rupture by shutting off steam flow to the reboiler
- On detecting high pressure, prevent tank rupture by opening valve to relief system
- On detecting high level, open drain valve to direct excess liquid to waste sump to reduce environmental damage
- On detecting a fire, issue alarms to minimize damage and possible injury

*Note: The last item is not a complete SIF since it does not achieve a safe state. The final actions must be included.*
What is SIL
SIL: Safety Integrity Level

“Discrete level (one out of four) for specifying the safety integrity requirements of the safety instrumented functions to be allocated to the safety instrumented systems. SIL 4 has the highest safety integrity and SIL 1 the lowest.”

*IEC 61511 Part 1 : 3.2.74*

How well the SIF performs its job of managing risk
Safety Lifecycle – IEC 61511

Management of Functional Safety and Functional Safety Assessment
Clause 5

Safety Lifecycle Structure and Planning
Clause 6.2

Analysis

Process Hazard & Risk Analysis [Clause 8]

Allocate Safety Function to Protection Layers [Clause 9]

SIS Safety Requirements Specification [Clauses 10 & 12]

SIS Design and Engineering [Clauses 11 & 12]

SIS FAT [Clause 13]

SIS Installation & Commissioning [Clause 14]

SIS Safety Validation [Clause 15]

SIS Operation & Maintenance [Clause 16]

SIS Modification [Clause 17]

SIS Decommissioning [Clause 18]

FEED

Concept

Design & Build

Test

Install

Validate

Proof Test

Manage

Verification

Clause 7 & Clause 12.7

March 11, 2014

Copyright © exida.com LLC 2000-2014
Analysis Phase

1. Process Design – Scope Definition
2. Identify Potential Hazards
3. Consequence Analysis
4. Identify Protection Layers
5. Likelihood Analysis (LOPA)
6. Select RRF, Target SIL for each SIF
7. Develop Process Safety Specification

IEC61511 Stage 1 FSA

March 11, 2014

Copyright © exida.com LLC 2000-2014
Safety Integrity Level Selection

Objective
- Specify the required risk reduction, or difference between existing and tolerable risk levels – in terms of SIL

Tasks
- Compare process risk against tolerable risk
- Use decision guidelines to select required risk reduction
- Document selection process

<table>
<thead>
<tr>
<th>Safety Integrity Level</th>
<th>Risk Reduction Factor</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIL 4</td>
<td>100000 to 10000</td>
</tr>
<tr>
<td>SIL 3</td>
<td>10000 to 1000</td>
</tr>
<tr>
<td>SIL 2</td>
<td>1000 to 100</td>
</tr>
<tr>
<td>SIL 1</td>
<td>100 to 10</td>
</tr>
</tbody>
</table>

IEC61511
ISA84.01

March 11, 2014
Copyright © exida.com LLC 2000-2014
• Objective
  – Specify all requirements of SIS needed for detailed engineering and process safety information purposes

• Tasks
  – Identify and describe safety instrumented functions
  – Document SIL
  – Document action taken – Logic, Cause and Effect Diagram, etc.
  – Document associated parameters – timing, maintenance/bypass requirements, etc.
Design Phase

8. SIF Conceptual Design
Select Technology

9. SIF Conceptual Design
Select Architecture

10. SIF Conceptual Design
Determine Test Plan

11. SIF Conceptual Design
Reliability / Safety Calc.

RRF, SIL Achieved?

NO

YES

12. Detailed Design

13. Factory Acceptance Test

IEC61511 Stage 2 FSA

Equipment Justification Report

H/W & S/W Design Safety Requirements

Detailed Design Documentation

FAT Test Report

Manufacturer Safety Manual
Application Standards

Manufacturer Safety Manual
Failure Rate Database

Manufacturer Safety Manual
Application Standards

Copyright © exida.com LLC 2000-2014
Operation and Maintenance Phase

1. Manufacturer’s Installation Instructions
2. Validation Plan
3. Security Regulation Guidelines
4. O&M Plans & Proof Test Procedures

Stage 4
- 14. SIS Installation & Commissioning
- Commission Test Report
- Validation Test Report
- Cyber-Security Audit Report
- Maintenance Records
- Proof Test Results

Stage 5
- Change Requests
- Safety Impact Analysis
- Change Authorizations

Stage 3 (Required)
- Change Authorizations

Back to appropriate SLC Step

19. SIS Decommissioning
Critical Issues

• Defines user project requirements well
• SIL Verification
• Proven-in-Use or IEC 61508 for ALL EQUIPMENT
• Requirements management
Defines user project requirements well

- Safety Lifecycle
- Strength against random failures
- Strength against systemic failure
SIF Verification Task

Safety Requirements Specification:
Safety Requirements including SIL target

Manufacturer Safety Manual
Failure Rate Database

11. SIF Conceptual Design
Reliability / Safety Calc.

PFDavg, RRF
MTTFS, SIL achieved
Select Technology

Objective

- Choose the right equipment for the purpose - all criteria used for process control still apply

Tasks

- Choose equipment
- Obtain reliability and safety data for the equipment
- Obtain Safety Manual for any safety certified equipment or equipment making a SIL capability claim
IEC 61511, Functional Safety for the Process Industries, requires that equipment used in safety instrumented systems be chosen based on either IEC 61508 assessment (parts 2 and 3) to the appropriate SIL level or justification based on “prior use” criteria (IEC 61511-1, 11.5.3)
Select Architecture

• Objective
  – Choose type of redundancy if needed

• Tasks
  – Choose architecture
  – Obtain reliability and safety data for the architecture
Establish Proof Test Frequency - Options

• In general the testing can include:
  – Automatic testing which is built into the SIS
  – Off-line testing, which is done manually while the process is not in operation
  – On-line testing, which is done manually while the process is in operation
Effects of Incomplete Testing

Because of incomplete testing the PFD never returns to its original value and the risk reduction can be significantly lower.
Compliance Requirements

SIL Capability

Architectural Constraints

Probability of Failure

Compliance
Importance of Data Integrity

- Why does it matter?
- Comparison of data sources
- Impact of “too good to be true” data
- Product Stewardship
- Legal Responsibility
Effect of Bad Data

• Optimistic data leads to unsafe designs
  – Insufficient redundancy
  – Insufficient testing

• Required risk reduction will not be reached
BAD Data

• Merriam-Webster defines BAD:
  – Failing to reach an acceptable standard: POOR < a bad repair job >

• exida defines BAD data as:
  – Data that leads to unrealistic, often dangerous, designs.
## Risk Varies With Use

<table>
<thead>
<tr>
<th>Use</th>
<th>Statement</th>
<th>Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Marketing Brochure</td>
<td>“We make very high quality stuff, it never fails!”</td>
<td>LOW: Reputation may suffer from exaggerated claims</td>
</tr>
<tr>
<td>Safety Reliability Calculations</td>
<td>“Look the math shows you don’t need redundancy and never need to test the function.”</td>
<td>VERY HIGH: Potential loss of life due to under-designed safety functions.</td>
</tr>
</tbody>
</table>
What are Some Companies Missing?

• One of the premises of IEC 61508 and IEC 61511 is that automated protection systems with diagnostics and periodic testing can provide higher safety reliability than typical control functions.

• The standards outline the steps that must take place to claim this higher safety reliability.

• However these steps are only valid if appropriate (GOOD) data is used.
Failure Rate Data Models

• Industry Databases
  – NOT Application Specific
  – NOT Product Specific

• Manufacturer FMEDA, Field Failure Study
  – Product Specific
  – NOT Application Specific

• Detail Field Failure Study – Application model
  – Product Specific
  – Application Specific
Mechanical Cycle Testing

Cycle Testing is useful for estimating failure rates when the dominant mechanical failure rates are due to (premature) wear-out of components. This occurs in applications with frequent dynamic movement, lubrication and mechanical loading. **Testing must be done until at least 10% of the population has failed.**

This method is **NOT APPLICABLE** to static applications such as demand mode safety systems as it does not account for failure modes like sticktion, cold welding, corrosion, etc.
Field Failure Studies

Field failure studies with sufficient information represent a rich opportunity to obtain failure rate and failure mode information about a product in a specific application.

- A problem is insufficient information. However, even limited information is useful.
- Manufacturer’s warranty studies are particularly bad as many failures are classified as “not a failure” and not counted.
FMEDA Based Failure Model

A predictive failure rate / failure mode model for some components can be constructed from a hierarchical set of FMEDAs. The component database is the repository of the data.
FMEDA = Validated Results

Proven In Use Study
- Performed for all assessments

FMEDA = 88 FITS
PIU = 57 FITS

Classified Failures

<table>
<thead>
<tr>
<th>Data</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Failures</td>
<td>69 failures reported</td>
</tr>
<tr>
<td>Total Operating Hours</td>
<td>2.43E+09 # devices x # years x 8760 hours/year</td>
</tr>
<tr>
<td>% Reported Failures</td>
<td>50% mix of expensive and inexpensive devices, warranty period</td>
</tr>
<tr>
<td>Estimate Actual Failures</td>
<td>138</td>
</tr>
<tr>
<td>Point Estimate - Failure Rate</td>
<td>5.67E-08</td>
</tr>
<tr>
<td>Complexity Factor</td>
<td>1 new versus old design if applicable</td>
</tr>
<tr>
<td>Estimate New Actual Failures</td>
<td>138 estimated failures of new design</td>
</tr>
<tr>
<td>New Point Estimate - Failure Rate</td>
<td>5.67E-08 per hour</td>
</tr>
<tr>
<td>Confidence Interval</td>
<td>0.7 IEC 61508, Part 2, 7.4.7.9</td>
</tr>
<tr>
<td>Upper Confidence Limit failure rate</td>
<td>5.93E-08 per hour</td>
</tr>
<tr>
<td>Lower Confidence Limit MTTF</td>
<td>1923.6 years</td>
</tr>
</tbody>
</table>

March 11, 2014

Copyright © exida.com LLC 2000-2014
Use Care with High Demand Certifications

Some certifications are based on failure data derived from “cycle testing” or other methods that require frequent movement of electro-mechanical products. This assessment is not valid for typical low demand process applications.

OEM has Product Stewardship Responsibilities. Don’t supply high demand data for low demand applications!

### Summary of the technical safety characteristics

<table>
<thead>
<tr>
<th>Probability of dangerous failure on demand</th>
<th>PFD_{spec}</th>
<th>Failure/demand</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test interval</td>
<td>Ti</td>
<td>y</td>
</tr>
<tr>
<td>Confidence interval</td>
<td>1-α</td>
<td>%</td>
</tr>
<tr>
<td>Safe failure fraction</td>
<td>SFF</td>
<td>%</td>
</tr>
<tr>
<td>Hardware fault tolerance</td>
<td>HFT</td>
<td>[-]</td>
</tr>
<tr>
<td>Diagnostic coverage</td>
<td>DC</td>
<td>%</td>
</tr>
<tr>
<td>Type of sub system</td>
<td>IEC 61508-2, 7.4.4.1.2</td>
<td>Type A</td>
</tr>
<tr>
<td>Mode of Operation</td>
<td>IEC 61508-4, 3.5.16</td>
<td>Low Demand Mode</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Assumed demands per year</th>
<th>f_{np}</th>
<th>demand/y</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interval for closing test</td>
<td>y</td>
<td>1</td>
</tr>
</tbody>
</table>

**Derived Values**

<table>
<thead>
<tr>
<th>Demand/hour</th>
<th>f_{np}</th>
<th>demand/h</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mean time between demands</td>
<td>h</td>
<td>10</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Dangerous failure rate</th>
<th>λ_D</th>
<th>1/h</th>
<th>8,54E-09</th>
</tr>
</thead>
<tbody>
<tr>
<td>MTBF dangerous failures</td>
<td>MTBF_{D}</td>
<td>h</td>
<td>1,17E+08</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Safe failure rate</th>
<th>λ_S</th>
<th>1/h</th>
<th>7,68E-08</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total failure rate</td>
<td>λ_S + λ_D</td>
<td>FIT</td>
<td>8,54E-08</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>MTBF total</th>
<th>h</th>
<th>1,17E+07</th>
</tr>
</thead>
<tbody>
<tr>
<td>MTBF total</td>
<td>y</td>
<td>1336,90</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Dangerous detected</th>
<th>λ_{DD}</th>
<th>1/h</th>
<th>0,00E+00</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dangerous undetected</td>
<td>λ_{DU}</td>
<td>1/h</td>
<td>8,54E-09</td>
</tr>
<tr>
<td>Safe detected</td>
<td>λ_{SD}</td>
<td>1/h</td>
<td>0,00E+00</td>
</tr>
<tr>
<td>Safe undetected</td>
<td>λ_{SU}</td>
<td>1/h</td>
<td>7,68E-08</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Average probability of failure on demand</th>
<th>PFD_{avg}</th>
<th>Failure/demand</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>3,74E-05</td>
<td></td>
</tr>
</tbody>
</table>

March 11, 2014
### Optimistic Data

#### Safety Instrumented Function Results

<table>
<thead>
<tr>
<th>MTTFs Contribution</th>
<th>PFDavg</th>
<th>MTTFs (years)</th>
<th>SIL PFDavg</th>
<th>SIL Limits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sensor Part</td>
<td>1.09E-03</td>
<td>384.78</td>
<td>2</td>
<td>N/A</td>
</tr>
<tr>
<td>Logic Solver Part</td>
<td>1.34E-04</td>
<td>7.43</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Final Element Part</td>
<td>6.35E-05</td>
<td>∞</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Achieved Safety Integrity Level**: 2
- **Safety Integrity Level (PFDavg)**: 2
- **Average Probability of Failure on Demand (PFDavg)**: 1.28E-08
- **Risk Reduction Factor (RRF)**: 760
- **Mean Time to Failure Spurious (MTTFs) [years]**: 7.29

#### Final Element is only 5% of total

- **12.1 FITS**
- **9458 years MTTF**

Function “achieves” SIL 2
- No diagnostics or redundancy
Realistic Data

![Diagram showing a flowchart with labeled elements]

**Final Element main contributor**

**Safety Instrumented Function Results**

- Achieved Safety Integrity Level: 1
- Safety Integrity Level (PFDavg): 1
- Average Probability of Failure on Demand (PFDavg): 2.74E-02
- Risk Reduction Factor (RRF): 37
- Mean Time to Failure Spurious (MTTFS) [years]: 7.03

**MTTFS Contribution**

<table>
<thead>
<tr>
<th>Component</th>
<th>PFDavg</th>
<th>MTTFS [years]</th>
<th>SIL PFDavg</th>
<th>SIL Limits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sensor Part</td>
<td>1.09E-03</td>
<td>384.78</td>
<td>1</td>
<td>N/A</td>
</tr>
<tr>
<td>Logic Solver Part</td>
<td>1.34E-04</td>
<td>7.43</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Final Element Part</td>
<td>2.62E-02</td>
<td>196.35</td>
<td>1</td>
<td>N/A</td>
</tr>
</tbody>
</table>

**1311 FITS**
87 years MTTF

**Improve reliability by implementing diagnostics**
Optimistic = Unsafe

“A SIS is defined as a system composed of sensors, logic solvers and final elements designed for the purpose of:

- 1. Automatically taking an industrial process to a safe state when specified conditions are violated;
- 2. Permit a process to move forward in a safe manner when specified conditions allow (permissive functions); or
- 3. Taking action to mitigate the consequences of an industrial hazard.”
Legal Responsibility

- Design Engineer – demonstrating reasonable level of expertise and judgment?
- EPC – Providing adequate training and controls?
- OEM – Supplying application appropriate information?
- Asset Owner – Implementing and maintaining an acceptable PSM program?
The Courts Will Decide

2 BP workers indicted on manslaughter counts in Deepwater Horizon oil spill

New Orleans – Two men who worked for BP during the 2010 oil spill disaster have been charged with manslaughter and with lying to federal investigators, according to indictments made public Thursday, hours after BP announced it was paying $4 billion in a settlement with the U.S. government over the disaster.

A federal indictment unsealed in New Orleans claims BP well leaders Robert Kaluza and Donald Vidrine acted negligently in the supervision of key safety tests performed on the Deepwater Horizon drilling rig before the explosion killed 11 workers in April 2010. The indictment says Kaluza and Vidrine failed to phon to offshore engineers onshore to alert them of problems in the drilling operation.

Buncefield verdict to renew focus on oil safety

The conclusion of a Buncefield prosecution this week comes at a difficult time for the oil industry.

Terry Macalister
The Guardian, Sunday 6 June 2010 12.45 EDT
Recent News

Toyota's killer firmware: Bad design and its consequences

Michael Dunn - October 28, 2013

News & Analysis

Acceleration Case: Jury Finds Toyota Liable

Junko Yoshida
10/24/2013 09:00 PM EDT
43 comments

It wasn't loose floor mats or a sticky pedal that caused the sudden acceleration of a 2005 Camry in an accident that killed one woman and seriously injured another on an Oklahoma highway off-ramp in September 2007. The electronic throttle control system did it.

This was the closing argument of the plaintiffs' attorneys. In contrast, attorneys for Toyota blamed the crash on driver error.

In a verdict delivered Thursday afternoon, an Oklahoma County jury found Toyota's in-car technology liable for the crash.

The Associated Press reports that the jury awarded $1.5 million in monetary damages to Jean Bookout, the driver of the car, who was injured in the crash, and $1.5 million to the family of Barbara Schwarz, who died. The jury also decided Toyota acted with "reckless disregard" for the rights of others. A second phase of the trial on punitive damages is scheduled to begin Friday.

Bellwether

Experts had viewed the Oklahoma case -- one of several hundred contending that the company's vehicles tended to accelerate inadvertently -- as a bellwether. This was the first test of a claim that put the fault squarely on a flaw in the vehicle's electronic throttle control system. Embedded systems experts who reviewed Toyota's electronic throttle source code testified that they found it defective. They said it contains bugs -- including some that can cause unintended acceleration.

It's important to note, however, that Toyota's electronics throttle control system had already been the subject of a NASA investigation that reportedly found no electronic causes of unintended acceleration. After the US space agency's 10-month investigation, the National Highway Traffic Safety Administration closed its probe of Toyota models in February 2011.
Product Certification
Safety Lifecycle – IEC 61508

“ANALYSIS” Phase

1. Concept
2. Overall Scope Definition
3. Hazard & Risk Analysis
4. Overall Safety Requirements
5. Safety Requirements Allocation

“REALIZATION” Phase

6. Overall Planning
7. Validation Planning
8. Installation & Commissioning Planning
9. Safety-related systems: E/E/PES Realization
10. Safety-related systems: other Technology Realization
11. External Risk Reduction Facilities Realization

“OPERATION” Phase

12. Overall Planning
13. Overall Installation & Commissioning
14. Overall Safety Validation
15. Overall Operation & Maintenance
16. Overall Modification & Retrofit
IEC 61508 – Fundamental Concepts

IEC61508 Safety Life Cycle – detailed engineering process

Probabilistic performance based system design

- Systematic Faults – Design Mistakes
- Random Failures
IEC 61508 Certification Milestones

1. Hardware - meet $PFD_{AVG}$ expectations for target SIL via:
   - Low failure rates, fail-safe design
   - High diagnostic coverage

2. Hardware - Meet SFF requirement for target SIL.

3. Software - Meet software process requirements for target SIL, systematic fault avoidance

4. Product - Meet design process requirements for target SIL, systematic fault avoidance

5. Produce Safety Manual for User
What does it mean for product development?

- Need a documented lifecycle for safety
- Need requirements for safety-related functions
- Need a safety-related validation plan
- Need a defined architecture
- Need a qualified set of tools including language compiler fit for the purpose
- Need a coding standard and documented description of other means utilized to qualify set of tools
- Need to follow the coding standard
- Need to verify compliance to coding standard, design requirements and other means
The end result of the certification process is a certificate listing the SIL level for which a product is qualified and the standards that were used for the certification.

A good certification assessment will demonstrate high design quality for hardware, software and high manufacturing quality.

A good certification assessment will check to see that proper end user documentation is provided – “The Safety Manual”
# Typical Project Documents

<table>
<thead>
<tr>
<th>Category</th>
<th>P/R</th>
<th>Preferred Document</th>
<th>FSM</th>
<th>P/R</th>
<th>Preferred Document</th>
</tr>
</thead>
<tbody>
<tr>
<td>FSM</td>
<td>1R</td>
<td>List of procedures</td>
<td>FSM</td>
<td>21P</td>
<td>Part Qualification Procedure</td>
</tr>
<tr>
<td>FSM</td>
<td>2P</td>
<td>Functional Safety Management Procedure</td>
<td>FSM</td>
<td>22P</td>
<td>Manufacturer qualification procedure</td>
</tr>
<tr>
<td>FSM</td>
<td>1P</td>
<td>Quality Management System Documentation Change Procedure</td>
<td>FSM</td>
<td>23P</td>
<td>Control of Design Documents</td>
</tr>
<tr>
<td>FSM</td>
<td>2R</td>
<td>Modification Procedure/Engineering Change Procedure</td>
<td>FSM</td>
<td>24P</td>
<td>Non-Conformance Reporting procedure</td>
</tr>
<tr>
<td>FSM</td>
<td>2R</td>
<td>Design Change Impact analysis</td>
<td>FSM</td>
<td>25P</td>
<td>Corrective Action Procedure</td>
</tr>
<tr>
<td>FSM</td>
<td>2P</td>
<td>Preventive Action Procedure</td>
<td>FSM</td>
<td>26P</td>
<td>Design Change Impact analysis</td>
</tr>
<tr>
<td>FSM</td>
<td>3R</td>
<td>IEC 61508 training record</td>
<td>FSM</td>
<td>27P</td>
<td>Preventive Action Procedure</td>
</tr>
<tr>
<td>FSM</td>
<td>3R</td>
<td>IEC 61508 training record</td>
<td>FSM</td>
<td>28P</td>
<td>Preventive Action Procedure</td>
</tr>
<tr>
<td>FSM</td>
<td>3R</td>
<td>Internall Audit Procedure</td>
<td>FSM</td>
<td>29P</td>
<td>Preventive Action Procedure</td>
</tr>
<tr>
<td>DSN</td>
<td>4R</td>
<td>Safety Requirements Specification</td>
<td>FSM</td>
<td>30P</td>
<td>Internal Audit Procedure</td>
</tr>
<tr>
<td>DSN</td>
<td>5R</td>
<td>Requirements review MOM/record</td>
<td>FSM</td>
<td>31P</td>
<td>Meeting minutes / Action Item list Tracking procedure</td>
</tr>
<tr>
<td>DSN</td>
<td>6R</td>
<td>FSM Plan</td>
<td>FSM</td>
<td>32P</td>
<td>Job descriptions /Competency Levels</td>
</tr>
<tr>
<td>DSN</td>
<td>7R</td>
<td>List of applicable agency standards</td>
<td>FSM</td>
<td>33P</td>
<td>Training Procedure</td>
</tr>
<tr>
<td>DSN</td>
<td>8R</td>
<td>Design Review MOM/record</td>
<td>FSM</td>
<td>34P</td>
<td>Training Record</td>
</tr>
<tr>
<td>DSN</td>
<td>9R</td>
<td>Gate Review and signoffs record</td>
<td>FSM</td>
<td>35R</td>
<td>Training Matrix</td>
</tr>
<tr>
<td>FSP</td>
<td>10R</td>
<td>Verification Plan</td>
<td>FSM</td>
<td>36R</td>
<td>IEC 61508 training record</td>
</tr>
<tr>
<td>FSP</td>
<td>11R</td>
<td>Verification Results</td>
<td>FSM</td>
<td>37P</td>
<td>Test equipment calibration procedure</td>
</tr>
<tr>
<td>DSN</td>
<td>12R</td>
<td>FMEDA</td>
<td>FSP</td>
<td>38P</td>
<td>Customer notification procedure for safety related products</td>
</tr>
<tr>
<td>INT</td>
<td>13R</td>
<td>Integration test plan</td>
<td>FSP</td>
<td>39R</td>
<td>ISO Cert</td>
</tr>
<tr>
<td>INT</td>
<td>14R</td>
<td>Intergration test results</td>
<td>OM</td>
<td>40R</td>
<td>Other applicable certs</td>
</tr>
<tr>
<td>FSP</td>
<td>15R</td>
<td>Validation Test Plan</td>
<td>OM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FSP</td>
<td>16R</td>
<td>Validation Test Plan Review MOM/record</td>
<td>OM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FSP</td>
<td>17R</td>
<td>Validation test results</td>
<td>OM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OM</td>
<td>18R</td>
<td>IOM manual</td>
<td>OM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OM</td>
<td>19R</td>
<td>Safety Manual</td>
<td>OM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OM</td>
<td>20R</td>
<td>Safety Manual review minutes/signoff</td>
<td>OM</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
exida Safety Case Database

Requirements

Arguments – Assessment

Audit Lists

Evidence
Main Product / Service Categories

Consulting
- Process Safety (IEC 61511)
- Control System Security (ISA S99)

Product Certification
- Functional Safety (IEC 61508)
- Functional Security
- Security Lifecycle
- Cyber-Security (ISASecure)

Training
- Process Safety
- Control System Security
- Onsite
- Offsite
- Web

Engineering Tools
- exSILentia
  - (PHAX HAZOP, SILAlarm, SIL Selection, LOPA, SRS, SIL Verification, Proof Tests)
- Safety Case
- FMEDA
- SCA

Reference Materials
- Databases
- Tutorials
- Textbooks
- Reference Books
- Market Studies

Professional Certification
- CFSE
- CFSP
- Control System Security Expert (CSSE)

www.cfse.org
excellence in dependable automation