How Safety And Safety Requirements Are Evolving In The Elevator Industry

November 28, 2012
DISCLAIMER/ TERMS OF USE:

THE INFORMATION PROVIDED HEREIN IS PROVIDED AS A GENERAL REFERENCE REGARDING THE USE OF THE APPLICABLE PRODUCTS IN GENERIC APPLICATIONS. THIS INFORMATION IS PROVIDED WITHOUT WARRANTY. IT IS YOUR RESPONSIBILITY TO ENSURE THAT YOU ARE USING ALL MENTIONED PRODUCTS PROPERLY IN YOUR SPECIFIC APPLICATION. ALTHOUGH THIS PRESENTATION STRIVES TO MAINTAIN ACCURATE AND RELEVANT INFORMATION, THERE IS NO OFFICIAL GUARANTEE THAT THE INFORMATION PROVIDED HEREIN IS ACCURATE. IF YOU USE THE INFORMATION PROVIDED HEREIN IN YOUR SPECIFIC APPLICATION, PLEASE DOUBLE CHECK ITS APPLICABILITY AND BE ADVISED THAT YOU ARE USING THIS INFORMATION AT YOUR OWN RISK. THE PURCHASER OF THE PRODUCT MUST CONFIRM THE SUITABILITY OF THE PRODUCT FOR THE INTENDED USE, AND ASSUME ALL RISK AND LIABILITY IN CONNECTION WITH THE USE.
Concerns Of Elevator Industry

General Public Transportation

Industrial Equipment
Developments In Industry

Elevator Industry

- Building markets still down
- Due to the down building markets, R&D Budgets also down
- Innovating and getting innovation to market quickly and efficiently is still critical

Industrial Automation

- Solid state programmable controls are increasingly prevalent
- Safety equipment is often integrated within a networked environment
- Safety controls incorporating solid state and programmable devices are more common, adding to the complexity
Industry Maintains A High Standard Of Safety

SAFETY FIRST

Innovation

Electronics

I/O system

Power supply

Processor

Communications device

Memory

Inputs

Outputs

Comm. link
How Requirements Can Accommodate Innovation

Electronic Protective Devices
• Safety Controls Specifically called out in Table 2.26.4.3.2 of ASME A17.1/CSA B44

• Requires that Electronic Protective Devices meet a specified Safety Integrity Level (SIL), as per IEC61508

Innovation
• ASME Performance Based Codes ASME A17.7/CSA B44.7

• Performance Based Code determines equivalent safety to requirements in ASME A17.1/B44
Electronic Controls

Table 2.26.4.3.2 allows use of Electronic Protective Devices in safety related control devices (Safety Integrity Level – SIL)

   Either positively opened, mechanically

   OR

   Listed / Certified / Marked with an IEC 61508 SIL level as appropriate

**Function** - When an EPD is activated, it shall provide an electronic function, removing electric power from the driving machine, motor and brake

**References**
ASME A17.1/CSA B44, Paragraphs 2.26.2, 2.26.4.3, 2.26.4.3.1, 2.26.4.3.2
Examples of safety related functions in ASME A17.1/CSA B44, Table 2.26.4.3.2

<table>
<thead>
<tr>
<th>Function</th>
<th>ASME A17.1/CSA B44 Reference</th>
<th>SIL Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unexpected Car Movement Device</td>
<td>2.26.2.34</td>
<td>3</td>
</tr>
<tr>
<td>Car Leveling or Truck Zoning Device</td>
<td>2.26.1.6</td>
<td>2</td>
</tr>
<tr>
<td>Firefighters stop switch</td>
<td>2.26.2.33</td>
<td>3</td>
</tr>
</tbody>
</table>
What is a SIL?

Safety Integrity Level (SIL) is defined as:
A relative level of risk-reduction provided by a safety function

In simple terms, SIL is a measurement of performance required for a Safety Instrumented Function (SIF).

<table>
<thead>
<tr>
<th>Risk Reduction Level</th>
<th>SIL</th>
</tr>
</thead>
<tbody>
<tr>
<td>LOWEST</td>
<td>1</td>
</tr>
<tr>
<td>↓</td>
<td>2</td>
</tr>
<tr>
<td>↓</td>
<td>3</td>
</tr>
<tr>
<td>HIGHEST</td>
<td>4</td>
</tr>
</tbody>
</table>
What if we have something that is specified in Table 2.26.4.3.2, how do we meet IEC 61508?


**Key concepts**

- **Functional Safety Management System** - Ensure that the full lifecycle management of a component, product or system incorporates the principles of FS
- **Reliability** – A product intended to ensure safe operation must be reliable commensurate with the risks
- **Fault Tolerant** – A product intended to ensure safe operation must be able to withstand faults proportionate with the risks
- **Environmental Resiliency** - Safety related systems shall withstand adverse environmental conditions corresponding with the risks and anticipated environment. Includes EMC.
Behind the SIL

• Failure Mode Effects Analysis (FMEA) or Failure Mode Effect Diagnostics Analysis (FMEDA)
  Evaluating the hardware and component failure rates

• Reviewing the design
  Hardware architecture can require redundancy or other methods of high reliability (diversity)

  Software architecture and programming methods are also subject to requirements

• Testing
  Fault insertion
  EMC testing (Identification of Common Cause Failures or CCFs)

• Process Review
  A quality product requires a quality process
V-Model and deliverables plan example for a E/E/PE (Sub-)system

- E/E/PES Safety Requirements Specification
  - E/E/PES Architecture Description
  - HW Architecture Description
  - Block-level FMEDA
  - SW Architecture Description
  - SW State machine diagram


- E/E/PES Test Specification and Report

- E/E/PES Integration Test Specification and Report

- HW Test specification and report
  - SW Test specification and report

- SW Module test specification and report
  - SW Criticality Analysis Report
  - SW Static Analysis Report

- SW Requirements Specification
  - SW Detailed Architecture
  - SW Detailed Design
  - SW Source Code

- HW Requirements Specification
  - HW Design documentation
  - Component-level FMEDA
  - PFH, SFF Calculation


- Functional Safety Plan, including Validation&Verification Plan

- Modification Procedure

Supporting Processes (EQM in fact)
Application Or Technologies That Do Not Fit “Nicely” Into ASME A17.1/CSA B44?

It may be an application → Wind Turbine Elevators do not fit “nicely” in ASME A17.1/CSA B44.

It may be an technology → Coated Steel Belts do not fit “nicely” in ASME A17.1/CSA B44.

Other unknown or unanticipated technologies, such as a Space Elevator, which is a combination of both an application and a technology that does not fit “nicely” in ASME A17.1/CSA B44.
What is the A17.7/CSA B44.7 performance based code process intended to achieve?

• Determine equivalent safety of new technologies based on performance
  • Equivalent to what? →
    • Requirements found in ASME A17.1/CSA B44

• Determined by who? →
  • An independent 3rd party, authorized by ANSI and / or SCC to issue AECO Certificates.

• How is Performance Determined? →
  • Risk Analysis, Engineering Analysis, Calculations, Testing, etc.
An Accredited Elevator/Escalator Certification Organization by
(ANSI) American National Standards Institute
or (SCC) Standards Council of Canada
based on ISO Guide 65
ASME A17.7/CSA B44.7 Is A Performance Based Code

Performance Based Safety Codes Encourage Innovation:

• Provides equivalent safety to current prescriptive codes
• Process is proactive rather than driven by accidents and mishaps
• Risk Assessment process systematically identifies and addresses the hazards
• This enables the development team to greatly reduce risks to users, non-users, authorized elevator personnel
• Compliance to performance based code is verified by an authorized third party (AECO)
The AECO Certification Process

Initial Review
More Info / Review CCD

Customer Develops Risk Assessment

AECO Reviews Determines Gap Analysis

Conduct Test

Issues Certification

AHJ Acceptance

Available for Public Use
Example

Alternate suspensions means
Risk Assessment (Manufacturers Process)

This process establishes the general principles and specific procedures for assessing risk.

Reference ISO 14798
# Lead with Severity!

<table>
<thead>
<tr>
<th>Severity</th>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>High</td>
<td>Death, system loss or severe environmental damage</td>
</tr>
<tr>
<td>2</td>
<td>Medium</td>
<td>Severe injury, severe occupational illness, major system or environmental damage</td>
</tr>
<tr>
<td>3</td>
<td>Low</td>
<td>Minor injury, minor occupational illness, minor system or environmental damage</td>
</tr>
<tr>
<td>4</td>
<td>Negligible</td>
<td>Will not result in injury, occupational illness, system or environmental damage</td>
</tr>
</tbody>
</table>
## Probability

<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Highly Probable</td>
<td>Likely to occur frequently</td>
</tr>
<tr>
<td>Probable</td>
<td>Likely to occur several times in the life cycle</td>
</tr>
<tr>
<td>Occasional</td>
<td>Likely to occur at least once in the life cycle</td>
</tr>
<tr>
<td>Remote</td>
<td>Unlikely, but may possibly occur in the life cycle</td>
</tr>
<tr>
<td>Improbable</td>
<td>Very unlikely to occur in the life cycle</td>
</tr>
<tr>
<td>Highly Improbable</td>
<td>Probability cannot be distinguished from zero</td>
</tr>
</tbody>
</table>
Estimate the risk

<table>
<thead>
<tr>
<th>Level of Probability</th>
<th>Level of Severity of the Effect (Harm)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1-High</td>
</tr>
<tr>
<td>A-Highly Probable</td>
<td>1A</td>
</tr>
<tr>
<td>B-Probable</td>
<td>1B</td>
</tr>
<tr>
<td>C-Occasional</td>
<td>1C</td>
</tr>
<tr>
<td>D-Remote</td>
<td>1D</td>
</tr>
<tr>
<td>E-Improbable</td>
<td>1E</td>
</tr>
<tr>
<td>F-Highly Improbable</td>
<td>1F</td>
</tr>
</tbody>
</table>
The AECO Certification Process

1. Initial Review
   - More Info / Review CCD

2. Customer Develops Risk Assessment

3. AECO Reviews Determines Gap Analysis

4. Conduct Test

5. Issues Certification

6. Available for Public Use

AHJ Acceptance

Underwriters Laboratories Inc.

AECO Certificate
Certificate No.: 1234567890123
Date: July 20, 2020

National Aeronautics and Space Administration (NASA)
For certification in accordance with the AISEL AS 7.7-2001 and SAE AS 314.7-07 of the following Elevator System

Space Elevator
Effective from: July 29, 2010 Until July 29, 2013
Questions?

For more information please feel free to contact us

Kevin Connelly
+1-631-546-2691
Kevin.Connelly@ul.com

Dan Posner
+1-631-546-2687
Daniel.Posner@ul.com