An Overview of Functional Safety for Automotive

November 2015
Unintentional Air Bag Deployment

Chevy recalls 2013 Malibu Eco over unintended airbag deployment fears

General Motors has announced the automaker is recalling certain 2013 Chevrolet Malibu models for a potential sensor failure. Under hard braking, the vehicle's sensing and diagnostic module may reset itself, and if that occurs just before an abrupt turn, the vehicle could trick itself into sensing a rollover. In that event, the roof rail airbag could deploy outside of a crash situation. What’s more, the seat belt pretensioners could then fail during a severe crash. Needless to say, it could be a dangerous situation. The recall covers a total of 4,304 units manufactured between October 24, 2011 and March 31, 2012.

Unintended Air-Bag Deployments Lead to Recall of 144,000 Ford F-150s

Ford is recalling about 144,000 F-150 pickups from the 2005-6 model years because the driver’s side air bag might deploy without the vehicle being in a crash, a Ford spokesman said Wednesday. The number represents a small fraction of the total F-150s that the National Highway Traffic Safety Administration was initially concerned about.

A defect investigation by the safety agency, which began late in 2009, grew eventually to cover about 1.3 million F-150s from the 2004-6 model years.

As a result of that investigation, the agency said it received 238 reports of “inadvertent deployment,” of which 77 resulted in injuries like abrasions, cuts, a broken tooth and, for two owners, loss of consciousness.

An air-bag wire in the truck’s steering wheel might have chafed against the horn plate’s metal edges, which could expose a bare copper wire “and create the potential for a short circuit that would illuminate the warning lamp,” Mr. Sherwood said. Left unfixed, the wire could, under “unique circumstances,” prompt the driver’s air bag to deploy.

Toyota Recalls RAV4 and Highlanders for faulty airbag sensors

Toyota announced a voluntary recall for almost 308,000 sport utility vehicles (SUV), more than three years after the auto maker learned that its curtain shield airbags could deploy without a crash.

Toyota has admitted to learning of the problem in 2007 and determined the cause to be a short circuit in two sensors. According to Toyota, the sensor design was changed in 2008. Despite the change, Toyota continued to receive reports of premature airbag deployments. Toyota did not consider the problem recall worthy because for the curtain shield airbag to deploy without a crash, it would require two short circuits to “occur nearly simultaneously after the initial air bag check.”

According to Toyota, they continued to monitor the situation. In March, Toyota change its position after a consumer was injured in a premature curtain shield deployment.

In 2010, Toyota was fined almost $49 million, the maximum allowed, from allegations by the National Highway Traffic Safety Administration (NHTSA) that the automaker had not reported safety problems in a timely manner.
Hackers Remotely Kill a Jeep on the Highway

Hackers send commands through the Jeep’s entertainment system to its dashboard functions, steering, brakes, and transmission, all from a laptop:

- the vents in the Jeep Cherokee started blasting cold air at the maximum setting
- Next the radio switched to the local hip hop station and began blaring Skee-lo at full volume
- windshield wipers turned on, and wiper fluid blurred the glass
- my accelerator stopped working
- functions that at lower speeds fully kill the engine, abruptly engage the brakes, or disable them altogether
- they cut the Jeep’s brakes, leaving me frantically pumping the pedal as the 2-ton SUV slid uncontrollably into a ditch
Safety Standards: Background

• The original designation of “engineer” was driven by safety

• The first role of an engineer was to ensure dangerous equipment (e.g., boilers, engines) would not fail with catastrophic results

• engineers followed technical standards for safe design of equipment

• Electronic controls in automobiles now perform safety-related functions

• Engineers must ensure electronic systems do not fail with catastrophic results

• ISO 26262 is the technical standard for safe design of such systems

kVA = engineered safety
What is ISO 26262?

- ISO 26262 is the *state of the art* standard for functional safety of E/E systems for passenger vehicles
  - Strongly intertwined with product development
  - Strong emphasis on functional safety management
  - Strong emphasis on the early phases of development
  - Requires traceability throughout entire lifecycle
  - *Not* a reliability standard
    - failures are allowed...
    - ...but prevention of a *safe state* is not

\[kVA = \text{engineered safety}\]
What is Automotive Functional Safety?

Layman’s Terms: Automotive functional safety is the desire to ensure that **malfunctions** of automotive **electronics and software** will not increase the risk of **injury or a fatality** above natural risks.

- Unintended acceleration (engine)
- Unintended shift (transmission)
- Sudden Loss of Steering Assist (Power Steering)
- Unintended Steering Column Lock (BMS)
- Unintended Steering (Steer-by-wire)
- Battery overcharge/overcurrent (BMS)
Vehicle's E/E systems are complex and are growing rapidly

### Platform Golf IV (1998)
- 17 ECUs
- 2 CANs
- 147 CAN-Messages
- 434 CAN signals

- Central Gateway
- 35 ECUs
- 5 CANs, 3 LINs
- 307 CAN-Messages
- 2669 CAN signals

### Platform Golf VI (2010)
- Central Gateway
- 49 ECUs
- 5 CANs, 7 LINs
- 704 CAN-Messages
- 6516 CAN signals


kVA = engineered safety
The Need for ISO 26262

Complex Vehicle Software Size (lines of code)

- F-22 Raptor: 1.7 Million
- F-35 Joint Strike Fighter: 5.7 Million
- Boeing 787 Dreamliner: 6.5 Million
- 2009 MB S-Class: 20 Million (radio and navigation only)
- ~100 Million (today) ~70-100 ECUs
- ~200-300 Million (predicted future)


kVA = engineered safety
1. Vocabulary

Part 2: Safety Management
Requirements related to the organization such as roles & responsibilities, safety culture, independent reviews, audits, and qualifications of personnel

Part 3: Safety Concept
A structured Hazard Analysis and Risk Assessment (HARA), leading to ASIL-rated safety goals
A concept for how to achieve safety in the product design

Part 4: Product Development at the System Level
Specification of safety requirements based on safety goals, and allocation to HW/SW elements
Integration and verification of safety functionality, culminating in formal assessment

Part 5: Hardware
Combination of best-practices and specific quantitative analysis to assure functional safety in hardware design
FMEDA, FTA, and similar analyses are critical to Part 5

Part 6: Software
Combination of best-practices and specific analysis to assure functional safety in software design
ASIL Tables, referencing best-practices and methods for SW assurance, are critical to part 6

Part 7: Production
Flow-through of functional safety concepts to the manufacturing floor
Change control, dedicated measures, supplier assessment & audit, etc.

Parts 8/9/10: “Other Useful Materials”
Norms, explanations, and reference concepts useful for implementing parts 2-7
**ISO 26262 Vocabulary**

**tolerable risk** → **Risk (1.99)** which is accepted in a given context based on the current moral concept of society.

**unreasonable risk** → **Risk (1.99)** judged to be unacceptable in a certain context according to valid societal moral concepts.
**safety** ➔ The absence of *unreasonable risk* (1.136).

**functional safety** ➔ Absence of unreasonable risk due to hazards caused by malfunctioning behaviour of E/E systems.
Legal Aspect

Product liability puts the burden of proof for acting with due care on the manufacturer. Therefore manufacturers must be able to provide evidence by appropriate documentation that they ensured the safety of its product with due care.

Reference: CTi ‘15, Functional safety new questions arise; Andreas Reuter
Legal Aspect

Trials deal with what you did 10 or 15 years ago...

- What can save you are:
  - Well defined processes *that were followed*
  - **Good documentation**

  "The dullest pencil is better than the sharpest memory."
  - Mark Twain

Reference: CTi ’15, U.S. Legal Issues – Overview and Practical Considerations; Clay Guise
Legal Aspect

How a standard can be used in U.S. Law

- Product **meets the standard**
- Standard applies but it **was not met**
- If standard had been met, product **would be “better”**
- Others do it “better” or “differently”

Reference: CTi ’15, U.S. Legal Issues – Overview and Practical Considerations; Clay Guise

kVA = engineered safety
## 1. Vocabulary

### 2. Management of functional safety

| 2-5 | Overall safety management |
| 2-6 | Safety management during the concept phase and the product development |
| 2-7 | Safety management after the item’s release for production |

### 3. Concept phase

| 3-5 | Item definition |
| 3-6 | Initiation of the safety lifecycle |
| 3-7 | Hazard analysis and risk assessment |
| 3-8 | Functional safety concept |

### 4. Product development at the system level

| 4-5 | Initiation of product development at the system level |
| 4-6 | Specification of the technical safety requirements |
| 4-7 | System design |

### 5. Product development at the hardware level

| 5-5 | Initiation of product development at the hardware level |
| 5-6 | Specification of hardware safety requirements |
| 5-7 | Hardware design |
| 5-8 | Evaluation of the hardware architectural metrics |
| 5-9 | Evaluation of the safety goal violations due to random hardware failures |
| 5-10 | Hardware integration and testing |

### 6. Product development at the software level

| 6-5 | Initiation of product development at the software level |
| 6-7 | Software architectural design |
| 6-8 | Software unit design and Implementation |
| 6-9 | Software unit testing |
| 6-10 | Software integration and testing |
| 6-11 | Verification of software safety requirements |

### 8. Supporting Processes

| 8-5 | Interfaces within distributed developments |
| 8-6 | Specification and Management of safety requirements |
| 8-7 | Configuration Management |
| 8-8 | Change Management |
| 8-9 | Verification |

| 8-10 | Documentation |
| 8-11 | Confidence in the use of SW tools |
| 8-12 | Qualification of SW Components |
| 8-13 | Qualification of HW Components |
| 8-14 | Proven in use argument |

### 9. ASIL-oriented and safety-oriented analyses

| 9-5 | Requirements Decomposition with respect to ASIL tailoring |
| 9-6 | Criteria for coexistence of elements |

| 9-7 | Analysis of dependent failures |
| 9-8 | Safety analyses |

### 10. Guideline on ISO 26262

15
ISO 26262 Part 3 Clause 7: Classification of Hazardous Events

Step 2 – For each hazard, what is the probability of the event?

Probability of Exposure

7.4.3.2 - The probability of exposure of each operational situation shall be estimated based on a defined rationale for each hazardous event. The probability of exposure shall be assigned to one of the probability classes, E0, E1, E2, E3 and E4, in accordance with Table 2.

<table>
<thead>
<tr>
<th>Description</th>
<th>E0</th>
<th>E1</th>
<th>E2</th>
<th>E3</th>
<th>E4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incredibly</td>
<td>Incredible</td>
<td>Very low probability</td>
<td>Low probability</td>
<td>Medium probability</td>
<td>High probability</td>
</tr>
</tbody>
</table>

kVA = engineered safety
Step 3 – For each hazard occurrence, how severe is the damage?

Severity

7.4.3.2 - The severity of potential harm shall be estimated based on a defined rationale for each hazardous event. The severity shall be assigned to one of the severity classes S0, S1, S2 or S3.

<table>
<thead>
<tr>
<th>Description</th>
<th>S0</th>
<th>S1</th>
<th>S2</th>
<th>S3</th>
</tr>
</thead>
<tbody>
<tr>
<td>No injuries</td>
<td>Light and moderate injuries</td>
<td>Severe and life-threatening injuries (survival probable)</td>
<td>Life-threatening injuries (survival uncertain), fatal injuries</td>
<td></td>
</tr>
</tbody>
</table>
Step 4 – For each hazard occurrence, to what degree can the situation be controlled, e.g. by the driver?

Controllability

7.4.3.2 - The controllability of each hazardous event, by the driver or other persons potentially at risk, shall be estimated based on a defined rationale for each hazardous event. The controllability shall be assigned to one of the controllability classes C0, C1, C2, and C3 in accordance with Table 3.

<table>
<thead>
<tr>
<th>Description</th>
<th>C0</th>
<th>C1</th>
<th>C2</th>
<th>C3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Controllable in general</td>
<td>Simply controllable</td>
<td>Normally controllable</td>
<td>Difficult to control or uncontrollable</td>
</tr>
</tbody>
</table>
ISO 26262 Part 3 Clause 7: ASIL Determination

- Based on the Hazard Assessment and Risk Analysis (HARA), each hazard is assigned an “Automotive Safety Integrity Level” or **ASIL**
  - Range from **ASIL A** (least stringent) to **ASIL D** (most stringent)
  - QM (Quality Management) follows normal development process
  - SAE J2980 released in May 2015 to harmonize levels

---

<table>
<thead>
<tr>
<th>Severity Class</th>
<th>Exposure Class</th>
<th>Controllability Class</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>C1</td>
</tr>
<tr>
<td>S1</td>
<td>E1</td>
<td>QM</td>
</tr>
<tr>
<td></td>
<td>E2</td>
<td>QM</td>
</tr>
<tr>
<td></td>
<td>E3</td>
<td>QM</td>
</tr>
<tr>
<td></td>
<td>E4</td>
<td>QM</td>
</tr>
<tr>
<td>S2</td>
<td>E1</td>
<td>QM</td>
</tr>
<tr>
<td></td>
<td>E2</td>
<td>QM</td>
</tr>
<tr>
<td></td>
<td>E3</td>
<td>QM</td>
</tr>
<tr>
<td></td>
<td>E4</td>
<td>A</td>
</tr>
<tr>
<td>S3</td>
<td>E1</td>
<td>QM</td>
</tr>
<tr>
<td></td>
<td>E2</td>
<td>QM</td>
</tr>
<tr>
<td></td>
<td>E3</td>
<td>A</td>
</tr>
<tr>
<td></td>
<td>E4</td>
<td>B</td>
</tr>
</tbody>
</table>

**kVA** = engineered safety
Scope of ISO 26262-4  Product development at the system level

- 4-5 Initiation of product development at system level
- 4-6 Specification of the technical safety requirements
- 4-7 System design
- 4-8 Item integration and testing
- 4-9 Safety validation
- 4-10 Functional safety assessment
- 4-11 Release for production

- 5 Product development Hardware level
- 6 Product development Software level

kVA = engineered safety
ISO 26262 Part 4 Clause 7.4.3: Measures for the avoidance of systematic failures

**systematic failure (1.130) → failure (1.39),** related in a deterministic way to a certain cause, that can only be eliminated by a change of the design or of the manufacturing process, operational procedures, documentation or other relevant factors

Systematic failure represents a design oversight or mistake

General methods to avoid systematic failure are called out by ISO 26262
ISO 26262 Part 4 Clause 7.4.4: Measures for control of random hardware failures

random hardware failure (1.192) → failure (1.39) that can occur unpredictably during the lifetime of a hardware element (1.32) and that follows a probability distribution.
ISO 26262 Part 5 Clauses 8 and 9: Random Hardware Failures & HW Architectural Metrics

ISO 26262-5:8 and ISO 26262-5:9 require specific metrics to be calculated, to demonstrate robustness of hardware against safety goal violation arising from random failure as follows:

<table>
<thead>
<tr>
<th>source</th>
<th>Requirement:</th>
<th>ASIL RATING</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO 26262-5, Table 4</td>
<td>Single-point fault metric</td>
<td>-</td>
</tr>
<tr>
<td>ISO 26262-5, Table 5</td>
<td>Latent-fault metric</td>
<td>-</td>
</tr>
<tr>
<td>ISO 26262-5, Table 6</td>
<td>Probabilistic Metric for HW Failure</td>
<td>-</td>
</tr>
</tbody>
</table>

One of several tools available to calculate these metrics: **FMEDA - Failure Modes, Effects, and Diagnostics Analysis**

**kVA = engineered safety**
ISO 26262 Part 5 Clauses 8 and 9: Random Hardware Failures & HW Architectural Metrics

Random Failures

Safety Mechanisms

A requirement of ISO 26262:

SPFM, LFM, PMHF

Several alternate approaches can meet the requirement:

Quantified FTA

failure rate classes (FRC) approach

kVA = engineered safety
Notes on Hardware Metrics and Targets

• The demands of ISO 26262-5, clauses 8 and 9 are severe, especially for ASIL C and ASIL D systems

<table>
<thead>
<tr>
<th>source</th>
<th>Requirement</th>
<th>ASIL RATING</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO 26262-5, Table 4</td>
<td>Single-point fault metric</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td></td>
<td>≥90%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>≥97%</td>
</tr>
<tr>
<td>ISO 26262-5, Table 5</td>
<td>Latent-fault metric</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td></td>
<td>≥60%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>≥80%</td>
</tr>
<tr>
<td>ISO 26262-5, Table 6</td>
<td>Probabilistic Metric for HW Failure</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&lt;10-7 /h</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&lt;10-7 /h</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&lt;10-8 /h</td>
</tr>
</tbody>
</table>

• Extensive hardware and software measures are typically required to achieve these challenging targets, such as
  – Lockstep processing
  – Memory partitioning and Intensive memory checking
  – CAN end-to-end protection
  – I/O monitoring
  – Plausibility checks

• Management Requirement: Assign responsibility for the safety analysis to determine these metrics, and ensure it is carried out

kVA = engineered safety
Software Development under ISO 26262

• Software failure is systematic by nature
  – Implication: failures are reduced, and safety is achieved, by careful and rigorous software process implementation

• A long list of methods are called out in ISO 26262, for all aspects of software development

• Most requirements are contained in so-called “ASIL Tables”
  – Provides lists of best practices for software development

kVA = engineered safety
ISO 26262 Part 6:
Product Development at the software level
## ISO 26262 Part 6 Clause 5:

**Initiation of product development at the software level**

### Top Ten Programming Languages According to IEEE

<table>
<thead>
<tr>
<th>Language Rank</th>
<th>Types</th>
<th>Spectrum Ranking</th>
<th>Spectrum Ranking</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Java</td>
<td>🌐📊📱</td>
<td>100.0</td>
<td>100.0</td>
</tr>
<tr>
<td>2. C</td>
<td>🌐📊📱</td>
<td>99.9</td>
<td>99.3</td>
</tr>
<tr>
<td>3. C++</td>
<td>🌐📊📱</td>
<td>99.4</td>
<td>95.5</td>
</tr>
<tr>
<td>4. Python</td>
<td>🌐📊📱</td>
<td>96.5</td>
<td>93.5</td>
</tr>
<tr>
<td>5. C#</td>
<td>🌐📊📱</td>
<td>91.3</td>
<td>92.4</td>
</tr>
<tr>
<td>6. R</td>
<td>🌐📊📱</td>
<td>84.8</td>
<td>84.8</td>
</tr>
<tr>
<td>7. PHP</td>
<td>🌐📊📱</td>
<td>84.5</td>
<td>84.5</td>
</tr>
<tr>
<td>8. JavaScript</td>
<td>🌐📊📱</td>
<td>83.0</td>
<td>78.9</td>
</tr>
<tr>
<td>9. Ruby</td>
<td>🌐📊📱</td>
<td>76.2</td>
<td>74.3</td>
</tr>
<tr>
<td>10. Matlab</td>
<td>🌐📊📱</td>
<td>72.4</td>
<td>72.8</td>
</tr>
</tbody>
</table>

**IEC 61508 Recommendations:**

- Not Recommended
- Highly Recommended with subset
- Not listed

*Posted July 20, 2015 by Stephen Cass on IEEE Spectrum*
Who is kVA?

- kVA is a technical consulting group based in the U.S., focused on **functional safety standards implementation**, with 3 U.S. locations:
  - Greensboro, NC
  - Greenville, SC
  - Royal Oak, MI

- kVA’s mission is to lead the implementation of functional safety standardization (**ISO 26262, IEC 61508, ISO 13849, + others**), in the U.S. and abroad

- kVA provides **training services, consulting and contract engineering services, audits and assessments, gap analysis**, and **engineering software** to enable functional safety at major automotive and industrial companies

\[ kVA = \text{engineered safety} \]
Introduction to kVA

kVA serves clients’ needs in:

- Functional Safety
- High Voltage Safety
- Electromagnetic Compatibility (EMC)
- Mechanical / Electrical Systems Integration
- Vehicle Architecture / Vehicle Design
- EV, PHEV, HEV, and ICE powertrains
- Diagnostics
- Regulatory Standards for Safety and Emissions
kVA is a Thought Leader in Vehicle Safety

- Served on the Safety Panel as functional safety expert at the IEEE International Electric Vehicle Conference in Greenville, April 2012
- Presented two technical papers on the topic of ISO 26262, related to BMS safety and EMC, at the 2013 SAE World Congress and Exposition in Detroit, April 2013.
- Two papers to be presented at the 2015 SAE World Congress
- CTI ISO 26262 Conference, Detroit
  - Conference Sponsor in June 2012
  - Conference Sponsor and Author in May 2013
  - Conference Sponsor in May 2014
- IQPC 26262 Conference, Ann Arbor
  - Conference Sponsor in September 2014

kVA = engineered safety
Contact

Jody J. Nelson
Managing Partner, kVA

Located in Greensboro, NC

jody.nelson@kvausa.com
786.999.8264

www.kvausa.com