VEHICLE SAFETY:
APPLICATION OF ISO26262 METHODOLOGY
LOTUS 414e SERIES HYBRID – ELECTRIC DRIVE SYSTEM

Automotive Electronics Systems Conference 2013 Sept 24th/25th University of Warwick

Presented by Chris Mahony CE Vehicle Control & Integration
Application of ISO 26262 Methodology

INTRODUCTION
Application of ISO 26262 Methodology

SUMMARY
Application of ISO 26262 Methodology

CONTENTS
- Background
  - Constraints, Concerns & why ISO 26262
- EDS Safety Concept Development
  - Item Definition, Hazard & Risk Analysis
- Safety Testing Development
  - Virtual Testing methods & Results
- Conclusion
- Questions
Application of ISO 26262 Methodology

BACKGROUND
414e HYBRID BACKGROUND

- The Lotus 414e R&D Concept Key Goals
- The 414e Commercial Constraints
- The 414e Design Constraints
414e HYBRID BACKGROUND

- Initial ‘Vehicle’ Safety Concerns

- Initial ‘Electric Drive System’ (EDS) Safety Concerns...
...Some Details:

- PM Motor inherent design
  - Normal Regen Torque

- What if a Motor Fault?
  - 2 or more phases ‘Short Circuit’ to chassis
  - Short Circuit Braking Torque

- What if a Power Electronics Fault?
  - 2 or more faults per leg

- Initial protection mitigation examples:
  - Fuse protection
  - Monitor motor short detection device

- Inappropriate example:
  - Contactors

---

![Short Circuit Torque & Current](chart)

<table>
<thead>
<tr>
<th>Torque (Nm)</th>
<th>Line Current (A)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>50</td>
<td>100</td>
</tr>
<tr>
<td>100</td>
<td>200</td>
</tr>
<tr>
<td>150</td>
<td>250</td>
</tr>
</tbody>
</table>

---

![Diagram](diagram)
Why did Lotus use the ISO 26262 approach?

- A methodology was required to demonstrate that the vehicle was safe to drive.

- Prior to this Standard

- Following this Standard
Application of ISO 26262 Methodology

EDS SAFETY CONCEPT
DEVELOPMENT
EDS SAFETY CONCEPT DEVELOPMENT

General Structure of ISO 26262

1. Vocabulary
2. Management of functional safety
   2.1 General safety management
   2.2 Safety management during item development
   2.3 Safety management after release for production
3. Concept phase
   3.1 Conceptual safety analysis
   3.2 Conceptual safety design
4. Product development: system level
   4.1 Development of product development at the system level
   4.2 Specification of systems safety requirements
   4.3 Safety analysis and risk assessment
5. Product development: hardware level
   5.1 Development of product development at the hardware level
   5.2 Specification of hardware safety requirements
   5.3 Hardware design
6. Product development: software level
   6.1 Development of product development at the software level
   6.2 Specification of software safety requirements
   6.3 Software design and implementation
   6.4 Safety validation
7. Production & Operation
   7.1 Production
   7.2 Operation, service and decommissioning
8. Supporting processes
   8.1 Documentation
   8.2 Certification of hardware components
   8.3 Certification of software components
   8.4 Certification of software integration
9. ASIL-oriented and safety-oriented analyses
   9.1 Requirements decomposition with respect to ASIL
   9.2 Safety analysis
10. (Informative) Guidelines on ISO 26262

ISO 26262 affects all areas
Item Definition

Summary of the **EDS**:

- **SUB-SYSTEM**: Traction Drive System (TDS)
- **FUNCTION**: Distribute power to the rear wheels
- **PURPOSE**: Applying correct power in driving scenarios to achieve desired torque levels.
ELECTRIC DRIVE SYSTEM

Consisting:

2x PM Traction Motors:
- 150kW 500Nm (peak)
- 75 kW 250Nm (nominal)

2 x single speed 4.587:1 Transmissions
ELECTRIC DRIVE SYSTEM

Combined:

Traction Drive System (TDS):

300kW 1000Nm (peak)
414PS (metric HP)
4600Nm at the Wheels
Item Definition

Summary of the EDS:

- **SUB-SYSTEM:** High Voltage Battery Pack
- **FUNCTION:** Electrical energy source & storage
- **PURPOSE:** Provide system power to meet vehicle performance demand.
ELECTRIC DRIVE SYSTEM

Consisting:

Electric Power Source:
Li-ion Pack 15kWhr 300kW
Capable of 1000A Discharge
Item Definition

Summary of the **EDS**:
- **SUB-SYSTEM**: **Vehicle Dynamics System**
- **FUNCTION**: Control Dynamic Functionality
- **PURPOSE**: Distribute controlled levels of torque to the twin electric motors and safety redundancy

- **SUB-SYSTEM**: **Lotus Vehicle Controller**
- **FUNCTION**: Propulsion system management
- **PURPOSE**: Control torque commands based on Energy Management and driver requests
ELECTRIC DRIVE SYSTEM

Consisting:

System Controllers:
1. Dynamics
2. Safety
3. Vehicle
The Hazard Analysis & Risk Assessment revealed the following:

- 40 Operational Scenarios
- 100+ Vehicle-Level Hazards identified
- Over 4000 possible ASIL rating
Relevant Risk Ratings revealed the following:

(Focused on the Worst Case Scenarios of the TDS)

- Loss of communications
- Short Circuit
- Cable or Insulation Breakdown

The highest for the EDS = D

<table>
<thead>
<tr>
<th>TOTAL</th>
<th>ASIL</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>D</td>
</tr>
<tr>
<td>18</td>
<td>C</td>
</tr>
<tr>
<td>47</td>
<td>B</td>
</tr>
<tr>
<td>8</td>
<td>A</td>
</tr>
<tr>
<td>16</td>
<td>No Rating</td>
</tr>
<tr>
<td>11</td>
<td>N/A</td>
</tr>
</tbody>
</table>

5.1.1 Summary

- Level D identified:
  - ASIL Risk on System Communication Interfacing (All)
  - ASIL Risk on HV Electric Shock (HV Battery, TDS)
  - ASIL Risk on HV Electric Discharge (HV Battery, TDS)
  - ASIL Risk on Thermal Runaway (HV Battery)
  - ASIL Risk on short circuits water immersion (TDS - Motors/Inverters)
  - ASIL Risk on cable/insulation breakdown (TDS - Motors/Inverters)
EDS Functional Safety Goals:

Example of goals:

- “Motor and Power Electronics Cable insulation should be robust throughout useful life against induced fatigue”

- “TDS Electronics should be robust throughout useful life against short-circuit caused by water immersion conditions identified within Life Targets”
EDS SAFETY CONCEPT DEVELOPMENT

General Structure of ISO 26262

1. Vocabulary
2. Management of functional safety
   2.1 Overall safety management
   2.2 Safety management during item development
   2.3 Safety management after release for production

3. Concept phase
   3.1 Item definition
   3.2 Initiation of the safety lifecycle
   3.3 Hazard analysis and risk assessment
   3.4 Functional safety concept

4. Product development: system level
   4.1 Initiation of product development at the system level
   4.2 Specification of the technical safety requirements
   4.3 System design
   4.4 System integration and testing

5. Product development: hardware level
   5.1 Product development at the hardware level
   5.2 Specification of immediate safety requirements
   5.3 Hardware architectural design
   5.4 Functional safety analysis of the hardware due to random failures
   5.5 Hardware integration and testing

6. Product development: software level
   6.1 Product development at the software level
   6.2 Specification of immediate safety requirements
   6.3 Software architectural design
   6.4 Software unit design and implementation
   6.5 Software integration and testing
   6.6 Software integration and testing
   6.7 Software validation

7. Production & Operation
   7.1 Production
   7.2 Operation, service and decommissioning

8. Supporting processes
   8.1 Documentation
   8.2 Certification of software tools
   8.3 Configuration management
   8.4 Change management
   8.5 Verification
   8.6 Validation

9. ASIL-oriented and safety-oriented analyses
   9.1 Requirements decomposition with respect to ASIL
   9.2 Analysis of system failures
   9.3 Safety analyses

10. (Informative) Guidelines on ISO 26262

Support
## EDS SAFETY CONCEPT DEVELOPMENT

### EDS Functional Safety Concept:

Safety Goals compliance and design using Functional Safety allocation Matrix:

- Thermal, Mechanical, Electrical, Software...

<table>
<thead>
<tr>
<th>ASIL Goals</th>
<th>50+ Design Sections</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detailed Requirement</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Compliance Matrix</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ingress Protection Standard</td>
</tr>
<tr>
<td>Fusing Specification</td>
</tr>
<tr>
<td>Cable Insulation</td>
</tr>
<tr>
<td>Earth Leakage Monitor</td>
</tr>
</tbody>
</table>

**Motor Short Circuit Safety Requirement examples...**
Application of ISO 26262 Methodology

EDS SAFETY TESTING

DEVELOPMENT
EDS SAFETY TESTING DEVELOPMENT

General Structure of ISO 26262

1. Vocabulary
2. Management of functional safety
   2.1 Overall safety management
   2.2 Safety management during item development
   2.3 Safety management after release for production
3. Concept phase
   3.1 Initiation of product development at the system level
   3.2 Initiation of the safety lifecycle
   3.3 Hazard analysis and risk assessment
   3.4 Functional safety concept
4. Product development: system level
   4.1 Specification of technical safety requirements
   4.2 System design
   4.3 Safety validation
   4.4 Functional safety assessment
   4.5 Release for production
5. Product development: hardware level
   5.1 Specification of product development at the hardware level
   5.2 Hazard analysis and risk assessment
   5.3 Hardware design
   5.4 Hardware architectural method
   5.5 Software safety and implementation
   5.6 Software integration and testing
6. Product development: software level
   6.1 Specification of software development at the software level
   6.2 Hazard analysis and risk assessment
   6.3 Software design and implementation
   6.4 Software integration and testing
   6.5 Software validation
7. Production & Operation
   7.1 Production
   7.2 Operational, service and decommissioning
8. Supporting processes
   8.1 Documentation
   8.2 Validation of hardware
   8.3 Configuration management
   8.4 Change management
   8.5 Verification
9. ASIL-oriented and safety-oriented analyses
   9.1 Safety analysis
   9.2 Hazard analysis
   9.3 Configuration analysis
10. (Informative) Guidelines on ISO 26262
Virtual Testing methods:

- IPG CarMaker environment developed for MiL Vehicle simulations
- Parameterised using modified Lotus Evora vehicle and driver models
- Short circuit motor torque provided by the motor designers
- Dynamic vehicle and driver simulations incorporating a model of the control systems
- Vehicle Model Correlation
Driving Scenario Testing:

- Identifies vehicle controllability

- Incorrect torques applied for Straight Line and Corner tests at various vehicle speeds

- Driver responses & Pass Fail Criteria

- Lotus Mitigation
Short Circuit Torques Test Results:

- 96 variations for each fault test insertion
- Unintended Straight line
- Unintended Corner

- In general the short circuit Torque conditions were far more controllable than first assumed
- Response worse with Regen Braking as mitigation
- Best counter measure is to Zero the unaffected motor torque (freewheel)
EDS SAFETY TESTING DEVELOPMENT

EDS HiL Testing Development:

- Further Safety Validation Testing
- TDS Lotus Test Cell validation
- Mixture of Real EDS Controllers

- Demonstrate safe operation for Torque Vectoring development phase
Application of ISO 26262 Methodology

CONCLUSION
Conclusions:

- Lotus successfully followed the ISO26262 methodology throughout the Functional Safety Concept and Development Activities.
- Initial Concerns with using twin PM Motors lead to Design mitigation being implemented and tested.
- During Development, extensive simulation testing was implemented on motor short circuit failures. The results conclude a further review in the reduction of future 414e EDS safety integrity levels.
Conclusions:
- During the application development, extensive use of the ISO 26262 Standard methodology lead Lotus to continually developing their in-house state-of-the-art Safety Tools.
- One of these being the AutoASIL Tool
THANK YOU FOR LISTENING
Please reply to:

<Chris Mahony>
Chief Engineer Vehicle Controls & Integration
+44 (0) 01953 608375
<cmahony@lotuscars.com>

Website: lotuscars.com/engineering