System Safety Process Applied to Automotive High Voltage Propulsion Systems

ISSC Tutorial
Mark Vernacchia, Galen Ressler, Padma Sundaram
August 2015
Tutorial Overview

- Objectives
- Safety Process Overview
- Safety Process Phases
- Safety Process Activities and Tools Applied to the Engineering Process
- Workshop Real Time Example
- Workshop Exercise Review
- Recap Summary
- Workshop Exercise Q&A

Many thanks to Sheila Schultz who helped create the initial tutorial package.
Tutorial Objectives

- Understanding of “What is a Safety-Critical System?”
- Understanding of System Safety and System Safety Process
- Understanding of Steps followed for an Automotive System Safety Process applied to a High Voltage Propulsion system
- Application to Real Examples
What are Safety-Critical Systems?

- Safety-critical systems are any systems where unintended behaviors could result in a potential safety concern under certain conditions.

- Example of Automotive Safety Critical Systems could include areas such as:
  - Steering and Braking
  - Propulsion
  - Active Safety Systems
What is System Safety?

- System Safety is a disciplined and comprehensive engineering effort to identify safety related risks to be either eliminated or controlled
  - It involves the identification of potential hazards, assessment of the risk, and mitigation of the risk to acceptable levels through design requirements
  - Analyzes the overall effect at the vehicle level including the operator and the environment as part of the system
  - Considers entire life cycle requirements including operation, maintenance and disposal phases where appropriate

- System can be comprised of software and hardware components. Each software and hardware component by itself can be safe, but interactions must also be analyzed.
System Safety Process Overview

- Modern automotive systems provide the benefits of enhanced vehicle functionality, fuel efficiency, safety, driver assistance, comfort, ride/handling, performance, and self-diagnostics.

- Modern automotive systems include: electrical/electronic sensors, embedded microcontrollers (processors), actuators, and communication devices.

- Typically these systems use complex software control algorithms made of many functions.

- Some of these systems are designed to autonomously activate independent of the user.
ISO26262

- ISO26262 - Functional Safety International Standard for Road Vehicles
- ISO26262 is an Adaptation of IEC 61508 (International Standard for Electrical, Electronic and Programmable Electronic Safety Related Systems) - to comply with the specific need of Electrical and Electronic systems within road vehicles.
A system safety process that follows the ISO26262 standard would:

- Provide early input to the system design by identifying potential hazards and determining the safety strategy
- Specify appropriate hardware (HW), software (SW), and interface requirements
- Confirm system content will satisfy these requirements
- Validate and verify system performance to requirements
- Document safety review and approval content
System Safety Process Phases (Provided as Example)

Supporting Processes
- Requirements Management
- Configuration and Change Control Management
- Quality Management
- Management of Development Tools / Reused components
- Safety Work products Retention

Concept
- Concept Changes

Requirements
- Requirement Changes

Design
- Design Corrections

Development / Implementation
- Design Corrections

Verification & Validation
- Production Observed Design Discrepancies

Production / Deployment
- Safety Verification / Validation
- Component, Sub-system, System, Vehicle
- FTA & DFMEA Verification
- System Safety Report & Assessment
- Production Safety Design & Test Review

Safety Functional Interface Analysis
- Translate Hazard Metrics into Engineering Requirements
- Safety Requirements Definition
- Safety V&V Planning
- Safety Requirements Review

Safety Concept
- Preliminary Hazard Analysis
- System Safety Program Planning
- System Safety Concept
- Single Element Fault Analysis
- Safety Concept Review

System / Component DFMEA
- System Level Fault Tree Analysis
- Common Cause Failure Analysis
- Refine / Update Safety Requirements
- Safety V&V Plan Update
- System Technical Safety Concept Update
- Safety Design Solution Review

System Safety Management

System Safety Tasks
- Preliminary Hazard Analysis
- System Safety Program Planning
- System Safety Concept
- Single Element Fault Analysis
- Safety Concept Review

 ISSC 2015

Concept

Requirements

Design

Development / Implementation

Verification & Validation

Production / Deployment

Supporting Processes
- Requirements Management
- Configuration and Change Control Management
- Quality Management
- Management of Development Tools / Reused components
- Safety Work products Retention

Safety Functional Interface Analysis
- Translate Hazard Metrics into Engineering Requirements
- Safety Requirements Definition
- Safety V&V Planning
- Safety Requirements Review

Safety Concept
- Preliminary Hazard Analysis
- System Safety Program Planning
- System Safety Concept
- Single Element Fault Analysis
- Safety Concept Review

System / Component DFMEA
- System Level Fault Tree Analysis
- Common Cause Failure Analysis
- Refine / Update Safety Requirements
- Safety V&V Plan Update
- System Technical Safety Concept Update
- Safety Design Solution Review

System Safety Management

System Safety Tasks
- Preliminary Hazard Analysis
- System Safety Program Planning
- System Safety Concept
- Single Element Fault Analysis
- Safety Concept Review

 ISSC 2015
System Safety Process Typical Phases

- The system safety process has a number of formal technical safety peer reviews that are conducted at critical milestones in the vehicle development process
  - Safety Concept Review
  - Safety Requirements Review
  - Safety Design Solution Review
  - Safety Design and Test Review

- These formal reviews have independent review board requirements and are intended to assess the safety process execution from a technical standpoint.
  - The formal reviews are intended to provide an independent assessment of the safety design and to confirm that the product satisfies the safety requirements.
System Engineering “V” Model

System Engineering “V” Model with Safety Phases

Initial Activity - Define System Scope and Content

- First, identify major vehicle systems and the interfaces between these systems
- Second, identify the safety-critical systems
- Third, determine scope boundary for the desired safety evaluation
Hazard Analysis and Risk Assessment (HARA)

Potential Hazards and Safety Goals

Hardware Integrity Requirements based on ASIL

High Level System Safety Requirements

Design Constraints

Final System State

Mitigation Action

Detection Method

Hazard (Y/N?)

Resulting State

Hardware Fault Analysis (System Element Hazard Analysis)

Lessons Learned from past and similar systems

Functional System Safety Concept: Intended safety strategy to satisfy the safety goals and safety requirements.
Safety Strategy Considerations

- Fail Safe or Fail Operational
- “Relative” Safe State Identification
  - Compared to more serious hazard states
- Typical Safe State Identification
- Mitigation and/or Prevention
- System Redundancy

**Safe State**: A system state with an acceptable risk
Assess Potential Hazards

- **A** hazard can be defined as any system state, event, or condition(s) that has the potential to cause physical harm to vehicle occupants and/or pedestrians.

- Hazard Analysis and Risk Assessment (HARA)
  - Systematically identify potential system hazards
  - Analyze mishap potential
  - Assess safety risk – using the ISO26262 ASIL (Automotive Safety Integrity Level) methodology is one approach
  - Determine of any Safety Goals
Risk Assessment

- Per ISO26262, Risk is expressed in terms of an **Automotive Safety Integrity Level (ASIL)**

- **ASIL** => function of (S, E, C)
  - S = Severity of the Hazard
  - E = Exposure likelihood to the operating scenario
  - C = Controllability of the operator/involved people

- Each of the factors have to be applied based on available data/statistics, **experience** and best **engineering judgment**

- ASIL specifies the developmental process rigor and the required hardware and software integrity requirements for the safety-critical system
For each identified hazard

1. Analyze the different operating scenarios: Consider normal driving conditions, maintenance/service and disposal phases
2. Identify the worst case severity potential for each identified hazard
3. Assess of operator will be able to prevent the hazard from becoming a mishap
4. Assign the ASIL
Driving Scenarios - Analysis

Consider:

- Normal Operation
- Degraded Operation with warning

Driving Situation

Road/Location Type
- High way/city road
- Off roads
- Parking lot
- Maintenance
- Garage

Road Conditions
- Surface friction
- Slope
- Road width (US vs. Europe)

Other Road Characteristics
- Side wind
- Oncoming traffic
- Traffic jam
- Construction zone
- Accident scenario

Driving Manœuvre
- Starting
- Turning (forward-reverse)
- Going straight (forward reverse)
- Parking
- Getting off

Driving State
- Coasting
- Stopped
- Accelerate
- Braking
- Parked
- Collision

Other Vehicle Characteristics
- State of other systems
- Ignition off/on
- Heavily laden
- Maintenance
- Driver capability
Perform a Hazard Analysis Determine ASIL

- For each identified hazardous scenario, evaluate …

<table>
<thead>
<tr>
<th>Severity</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>

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

<table>
<thead>
<tr>
<th>Controllability</th>
<th>C0</th>
<th>C1</th>
<th>C2</th>
<th>C3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Controllable in general</td>
<td>Simply controllable</td>
<td>Normally controllable</td>
<td>Difficult to control or uncontrollable</td>
<td></td>
</tr>
</tbody>
</table>

Source ISO 26262
### Risk Matrix with ASIL (based on ISO 26262)

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

QM = Quality Managed

Source: ISO 26262
Define Required Design Rigor and Integrity

- The ASIL rating drives process rigor and design integrity
  - Higher ASIL level equates to higher/more diagnostic capability

- Determine the diagnostic content needed to detect memory corruption or hardware failure to meet the requirements specified by the ASIL rating
  - Detect system faults and take required remedial action to transition to a “safe state” where the hazardous condition is eliminated
  - Examples of remedial actions include reduced performance or propulsion shut down
  - Develop a diagnostic strategy and implement diagnostic content which will detect and mitigate as required

- Once integrity requirements are determined, system level interface analysis tasks may be started
Perform System Level Interface Analysis

- Create a system “Control Structure” (Block Diagram)
- Identify functional requirements for each entity
- Determine information required between entities
- Identify system functional behavior and its interactions with other systems in the vehicle
- Define functional interactions among system entities
  - Different subsystems
  - Different control modules within the system
  - Sensors outputs
  - System actuator behaviors
Perform System Element Hazard Analysis

- System level fault analysis of the subsystems, controllers and modules can support identification of critical components of the system.

- Determine how system will behave when different portions of the system fail under different operating scenarios.
  - Performed at a high level (system vs. component).
  - Fail one entity at a time and determine effect on system.

- Determine how system will behave under different operating scenarios.
  - Engine provided vs. electric machine provided propulsion modes.
  - Park vs. Reverse vs. Neutral vs. Drive.

- Define safety hazards that may appear when fault(s) occur.

- Outline the initial diagnostic and mitigation strategies.

- Define the resulting “safe” system state.

- Identify the need for additional sensors, diagnostic SW, or required changes to system safety strategy so that critical component faults do not lead to potential safety hazards.
Perform Hazard Operability Analysis (HAZOP)

- Define Unsafe Control Actions (UCA) by using guidewords such as:
  - Not Provided
  - Provided but Incorrect
  - Too Early, Too Late
  - Frozen/Stuck

- Develop potential causes for each UCA

- Define design constraints (requirements) to prevent and/or minimize potential causes

Multiple system engineering based processes may be utilized for this step. MIT’s STPA is an example of such a process.
System Engineering “V” Model with Safety Phases

ISO26262 Standard

- ISO26262 provides information regarding Hardware and Software development efforts
  - **Hardware**
    - Controller Architecture
    - Memory Diagnostic Strategies
    - Software Redundancy Options
  - **Software**
    - Mechanisms for Error Detection
    - Mechanisms for Error Handling
Controller Architecture

- Safety requirement may drive the use of redundant processor architecture to ensure that certain faults do not lead to a hazard

- Delayed Dual Core Lock-Step Processor Architecture
  - Two physical cores that act as one logical core (not seen by software and does not provide additional throughput) where the outputs (calculations) of both of these cores is compared against each other to detect single point failures
  - The delay of one of the cores allows the comparison hardware to detect errors caused by external sources such as Power Supply Noise and Ionizing Radiation

- Leverage the diagnostic capabilities of this architecture to shift from software diagnostic to hardware diagnostic capability which reduces code development and testing
Memory Diagnostic Strategies

- RAM, ROM, flash, cache, stack, and Registers
- Detect and correct erroneous memory errors
  - ECC: Error-Correcting Code protection
    - Single bit errors are detected and corrected
    - Most multi-bit errors are detected
  - CRC
    - Cyclic Redundancy Check protection - checksum
- Parity check
  - Parity bit – bit encoding of there being an even or odd number of bits set to 1
  - Detects single bit errors
- Dual store – Redundant storage of safety critical variables
- Register Configuration Check

- End-to-End (E2E) ECC - Reduces number of circuits w/o ECC protection
  - Increased detectability and robustness from processor faults
  - Protect the address lines to memory
  - Integrate ECC encoders and decoders into the CPU cores
Software Redundancy Options

Rationalize Outputs with Forward Redundancy

Primary Control
\( (Y = HX) \)

Outputs: \( Y \)

Redundant Safety
\( (Y' = HX') \)

Outpus: \( Y' \)

Error

Maturing Filter

Fault

Inputs: \( X \)

Outputs: \( Y \)

Rationalize Inputs with Backwards (Inverse) Redundancy

Primary Control
\( (Y = HX) \)

Inputs: \( X \)

Outputs: \( Y \)

Redundant Safety
\( (X' = H^{-1}Y') \)

Inputs: \( X' \)

Outputs: \( Y' \)

Fault

Maturing Filter

Error

X≈X'
Latent Faults Require Special Care

- Latent Failures are benign faults until another fault occurs
- Identified and managed through rigorous engineering process so they are detected and managed appropriately

Concept
Requirements
Design
Development / Implementation
Verification & Validation
Allocate Safety Requirements to Engineering and Sourcing Documents

➢ Determine which engineering groups need to know about these requirements

➢ Communicate the requirements to these groups

➢ Confirm requirements have been accommodated in external sourcing documents and internal engineering specifications
Requirement Summary and Allocation

- Control Structure
- HARA Feedback
- HAZOP Analysis
- System Level Interface Analysis
- System Level Fault Analysis
- Regulatory Requirements
- Hardware Integrity Requirements
- Other Documents...

System Safety Requirements

- Functional Subsystem
  - High voltage
  - Contactors
  - Diagnostics
  - Software Components

- Physical Subsystem
  - Housing Cells
  - Electrical Electronics Module
  - Physical Components
System Engrg “V” Model with Safety Phases

System Design and Analysis Tasks

- DFMEAs (Design Failure Modes and Effects Analysis)
- SW Safety Analysis (HAZOP – SAE ARP-5580)
- FTA (Fault Tree Analysis)
- CCA – (Common Cause Analysis) – identify of potential common cause failures
Produce 1st Pre-Prototype Unit and Initial SW

- Early controller Electronic Controller hardware (Advanced technical work or early program work)

- Controller designed to requirements developed in Requirements phase

- Initial Safety Testing, Safe Usage, and Education
  - Have potential hazards identified
  - Install any required Mitigation Mechanism(s). Test the mitigation mechanism to ensure it operates as expected.
  - Until mature well tested SW is available, limiting driver usage and locations may be an appropriate action
  - Driver education regarding expected vehicle performance is helpful
Produce 1st Prototype Unit and Initial SW

- Confirm Hazard Metric(s)
- Simulate potential system hazardous states in early development vehicle and verify that the fault response times and the remedial actions designed in the system are acceptable to mitigate the hazard

- Depending on the fidelity of the early hardware, this may need to be performed when higher fidelity hardware becomes available
System Engineering “V” Model with Safety Phases

Produce 1st Prototype HW Unit and Beta SW

- “Beta” level controller hardware (more refined hardware) in a further refined development vehicle – Mule vehicle

- Controller may have been updated to comprehend further developed requirements learned through the early hardware phase

- Simulate potential system hazardous states in design intent vehicle and verify that the fault response times and the remedial actions designed in the system are acceptable to mitigate the hazard
Test 1<sup>st</sup> Production Intent HW Unit and SW

- Verify performance, correlation, and torque safety diagnostics are implemented properly
- System control content should be mature enough to allow the system to execute planned remedial actions
- Perform testing that exercises the interfaces between the vehicle’s safety critical systems
System Engrg “V” Model with Safety Phases

Perform Final Vehicle Safety Validation Testing

- Production Level Testing
- Final Bench and Vehicle Testing
- Execute/Complete testing to confirm system meets Safety Requirements
- Confirm no deficiencies in system safety / diagnostics
- “Avoid False Fails”
- Robustness
Document Safety Validation Results

- Complete execution of testing to verify and validate safety requirements
- Document testing results in a Validation Report
- Trace validation testing completion to requirements
Document Safety Validation Results

- **PHA Safety Concept**: PHA (Principles of Hazard Analysis)
- **System Safety Requirements**: System-level safety requirements
- **Functional Subsystem**: High voltage, Contactors, Diagnostics, Software Components
- **Physical Subsystem**: Housing Cells, Electrical Electronics Module, Physical Components

- **Safety Goals Achieved**: Results of the validation process

- **System Validation**: Verification of the system's safety goals
- **Functional Subsystem Verification**: Verification of functional subsystems
- **Physical Subsystem Verification**: Verification of physical subsystems

- **Component Verification**: Detailed verification of individual components

- **Safety Goals Achieved**: Final validation results
Create Safety Case

- A Safety Case is a document that provides convincing and valid argument that the system is acceptably safe for a given application in a given environment.
- System safety steps conducted progressively (system safety process steps)

- Safety Case addresses:
  - Does system satisfy technical system safety requirements?
  - Are standard processes carried out?
  - Are the System Safety Engineering Process steps carried out correctly?
  - Are all identified system safety related issues over the course of product development addressed and resolved?

- Stored and retained according to document retention policies
Questions Before We Take a Break  ???
And . . . . Let’s Take a Break
Welcome Back . . . .

Let’s apply what we discussed to a working example . . . .
System Content Example Illustration

Additional Radiator
Plug-In Socket
Electric Fan
Electric Drive Motor
Clutch Actuator
El. Vacuum Pump
HV el. AC-Compressor
El. Steering Pump
HV - Harness
Charger
Inverter
DC/DC Converter
HV-PDU
HV - Battery
System Content – Safety Critical Areas

- Accelerator Pedal Assembly
- 12V Battery
- Engine
- Engine Control Module
- Motor Control Module
- Electric Machines
- HV Battery
- Power Inverter Module
System Content – Power and Communication

- Accelerator Pedal Assembly
- Engine Control Module
- 12V Battery
- Motor Control Module
- Electric Machines
- HV Battery
- Power Inverter Module
- HV DC Power
- HV AC Power
- OUTPUT TORQUE
- 12V Power
- Communication Path

Reproduction or Reuse of this Material is Prohibited without Express Permission from GM

ISSC 2015
Workshop Example Possible Answers

Assess Potential Hazards

<table>
<thead>
<tr>
<th>HV Hazards</th>
<th>Vehicle Motion Hazards</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Different Operation Scenarios

- XXX
- XXX
Workshop Example Possible Answers

- **Assess Potential Hazards**

<table>
<thead>
<tr>
<th>HV Hazards</th>
<th>Vehicle Motion Hazards</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shock</td>
<td>Acceleration</td>
</tr>
<tr>
<td>Burn</td>
<td>Deceleration</td>
</tr>
<tr>
<td>Heat</td>
<td>Direction</td>
</tr>
</tbody>
</table>

- **Different Operating Scenarios**
  - Driving
  - Charging
  - Service
  - Crash
  - Towing
Workshop Example Possible Answers

- Rating Potential Hazards (High, Medium, or Low)

<table>
<thead>
<tr>
<th>HV Hazards</th>
<th>Vehicle Motion Hazards</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shock</td>
<td>Acceleration</td>
</tr>
<tr>
<td>Burn</td>
<td>Deceleration</td>
</tr>
<tr>
<td>Heat</td>
<td>Direction</td>
</tr>
</tbody>
</table>

- Result of Severity, Exposure, and Controllability

- High => ASIL ???
- Medium => ASIL ???
- Low => ASIL ???
Example ASIL Determination

<table>
<thead>
<tr>
<th>Hazard</th>
<th>Operating Scenario</th>
<th>Severity</th>
<th>Controllability</th>
<th>Exposure</th>
<th>ASIL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shock</td>
<td>Driving</td>
<td>S3</td>
<td>C3</td>
<td>E4</td>
<td>D</td>
</tr>
<tr>
<td></td>
<td>Crash</td>
<td>S3</td>
<td>C3</td>
<td>E2</td>
<td>B</td>
</tr>
<tr>
<td></td>
<td>Service</td>
<td>S3</td>
<td>C2</td>
<td>E3</td>
<td>B</td>
</tr>
</tbody>
</table>

**Severity**

- **S0**: No injuries
- **S1**: Light and moderate injuries
- **S2**: Severe and life-threatening injuries (survival probable)
- **S3**: Life-threatening injuries (survival uncertain), fatal injuries

**Exposure**

- **E0**: Incredible
- **E1**: Very low probability
- **E2**: Low probability
- **E3**: Medium probability
- **E4**: High probability

**Controllability**

- **C0**: Controllable in general
- **C1**: Simply controllable
- **C2**: Normally controllable
- **C3**: Difficult to control or uncontrollable
Workshop Example Possible Answers

- Rating Potential Hazards (High, Medium, or Low)

<table>
<thead>
<tr>
<th>HV Hazards</th>
<th>Vehicle Motion Hazards</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shock - High</td>
<td>Acceleration - High</td>
</tr>
<tr>
<td>Burn - Medium</td>
<td>Deceleration - Medium</td>
</tr>
<tr>
<td>Heat - High</td>
<td>Direction - Medium</td>
</tr>
</tbody>
</table>

- Result of Severity, Exposure, and Controllability (S, E, C)

- High => ASIL C and D
- Medium => ASIL B
- Low => ASIL A
## Workshop Example Possible Answers

### Diagnostic Integrity Requirements **

<table>
<thead>
<tr>
<th>HV and Motion Hazards</th>
<th>Single Point</th>
<th>Dual Point</th>
<th>Safety Metric</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shock - High</td>
<td>High</td>
<td>High</td>
<td>HV Metric</td>
</tr>
<tr>
<td>Burn - Medium</td>
<td>High</td>
<td>Medium</td>
<td>Burn Metric</td>
</tr>
<tr>
<td>Heat - High</td>
<td>High</td>
<td>High</td>
<td>Thermal Metric</td>
</tr>
<tr>
<td>Acceleration - High</td>
<td>High</td>
<td>High</td>
<td>Accel Metric</td>
</tr>
<tr>
<td>Deceleration - Medium</td>
<td>High</td>
<td>Medium</td>
<td>Decel Metric</td>
</tr>
<tr>
<td>Direction - Medium</td>
<td>High</td>
<td>Medium</td>
<td>Direction Metric</td>
</tr>
</tbody>
</table>

** Consult ISO-26262 Part 5 for Diagnostic Integrity Details
Safety Strategy

- **Fail Safe or Fail Operational**
  - Fail Safe – HV and Propulsion
  - Fail Operational – Steering and Brakes

- **Relative Safe State Identification**
  - Remedial actions that lead to a “lower” ASIL state should only be used as a “safe state” alternative to more severe safety hazards
  - Loss of Propulsion (Low) versus Unintended Acceleration (High)

- **Typical Safe State Identification**
  - Secured vehicle (immobile)
  - Reduced performance

- **Mitigation and/or Prevention**
  - Design Options to Eliminate Potential Issues
  - Mitigation Tactics that Achieve Safe States

- **System Redundancy**
  - Alternate Batteries
  - Reduced Propulsion Modes
System Control Structure

- **Driver**:
  - Vehicle Motion Desire
  - Engine Power Commands
  - Engine Feedback

- **Engine Control Module**:
  - Acceleration Pedal Sensor Input
  - Power Coordination Communication

- **Motor Control Module**:
  - Electric Motor Resolver Input
  - Power Inverter Module
    - Electric Motor Feedback
    - Electric Machine and Inverter Feedback

- **Power Inverter Module**:
  - Electric Power Commands
  - 3φ Motor Currents
  - Electric Motor Feedback
  - Back EMF Energy

- **Electric Machines**:
  - Electric Torque to Driveline
  - HV Supply Voltage

- **HV Battery**:
  - Recharge Voltage
  - HV Insulation and Isolation

- **Environmental Feedback Factors**:
  - IC Engine Torque to Driveline
  - Visceral Vehicle Motion Feedback

- **Vehicle Motion**:
  - HV Insulation and Isolation

**System Control Structure**

- **Accelerator Pedal Assembly**
- **HV Supply Voltage**
- **Recharge Voltage**
- **HV Insulation and Isolation**
- **IC Engine**
- **Electric Machines**
- **Vehicle Motion**
- **Power Coordination Communication**
- **Electric Power Commands**
- **Engine Feedback**
- **Engine Control Module**
- **Motor Control Module**
- **Power Inverter Module**
- **3φ Motor Currents**
- **Electric Motor Feedback**
- **Back EMF Energy**
- **HV Supply Voltage**
- **Recharge Voltage**
- **HV Insulation and Isolation**

**Workshop Tutorials**

**ISSC 2015**
High Level System Element Hazard Analysis

- Fault Analysis Results

<table>
<thead>
<tr>
<th>HV / Motion Hazards</th>
<th>Detection</th>
<th>Mitigation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shock - High</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Burn - Medium</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Heat - High</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Acceleration - High</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Deceleration - Medium</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Direction - Medium</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Primary Fault</td>
<td>Resulting Fault</td>
<td>Resulting State</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------</td>
<td>-----------------------------------------</td>
</tr>
<tr>
<td>Normal Operation</td>
<td>1 1 1 1 1 1 1 1 1 1 1 1</td>
<td>System Working Properly</td>
</tr>
<tr>
<td>Accel Pedal Assembly</td>
<td>0 1 1 1 1 1 1 1 1 1 1 1</td>
<td>Accel Pedal Assembly Fails Unsecured accel request possible Drive Intent Not Known</td>
</tr>
<tr>
<td>12V Battery Power</td>
<td>1 0 0 0 0 1 1 0 1 1 1 0</td>
<td>All controllers fail &lt;OFF&gt;</td>
</tr>
<tr>
<td>Engine Control Module</td>
<td>1 1 0 0 1 1 1 1 1 1 1 1</td>
<td>ECM Fails &lt;OFF&gt; IC Engine Shutdown</td>
</tr>
<tr>
<td>IC Engine</td>
<td>1 1 1 0 1 1 1 1 1 1 1 1</td>
<td>IC Engine Shutdown</td>
</tr>
<tr>
<td>Motor Control Module</td>
<td>1 1 1 1 0 0 0 1 1 1 1 1</td>
<td>MCM Fails &lt;OFF&gt; Electric Motor Shutdown</td>
</tr>
<tr>
<td>Electric Machine</td>
<td>1 1 1 1 0 1 1 1 1 1 1 1</td>
<td>Electric Motor Shutdown</td>
</tr>
</tbody>
</table>
## High Level System Element Hazard Analysis

<table>
<thead>
<tr>
<th>Resulting State</th>
<th>Safety Hazard Present?</th>
<th>How Detected?</th>
<th>Mitigation Strategy</th>
<th>Final Vehicle State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Normal Operation</td>
<td>System Working Properly</td>
<td>No</td>
<td>NA</td>
<td>Normal Operation</td>
</tr>
<tr>
<td>Accelerator Pedal Assembly</td>
<td>Accel Pedal Assembly Fails Unsecured accel request possible Drive Intent Not Known</td>
<td>HIGH Unintended Longitudinal Motion</td>
<td>ECM diagnostics of Accel Pedal sensor</td>
<td>ECM commands IC Engine shutdown and vehicle transitions to EV mode Driver warning provided</td>
</tr>
<tr>
<td>12V Battery Power</td>
<td>All controllers fail &lt;OFF&gt;</td>
<td>LOW Loss of Propulsion</td>
<td>Not Able to Detect by Diagnostics</td>
<td>No Mitigation Strategy Possible Vehicle Propulsion Shuts Down</td>
</tr>
<tr>
<td>Engine Control Module</td>
<td>ECM Fails &lt;OFF&gt; IC Engine Shutdown</td>
<td>LOW Loss of Propulsion</td>
<td>Other Controllers detect ECM failure thru CAN diagnostics</td>
<td>Vehicle transitions to EV mode Driver warning provided</td>
</tr>
<tr>
<td>IC Engine</td>
<td>IC Engine Shutdown</td>
<td>LOW Loss of Propulsion</td>
<td>ECM diagnostics of Engine sensors</td>
<td>Vehicle transitions to EV mode Driver warning provided</td>
</tr>
<tr>
<td>Motor Control Module</td>
<td>MCM Fails &lt;OFF&gt; Electric Motor Shutdown</td>
<td>LOW Loss of Propulsion</td>
<td>Other Controllers detect MCM failure thru CAN diagnostics</td>
<td>Vehicle transitions to IC Engine mode Driver warning provided</td>
</tr>
<tr>
<td>Electric Machine</td>
<td>Electric Motor Shutdown</td>
<td>LOW Loss of Propulsion</td>
<td>MCM readings of Resolver sensors</td>
<td>Vehicle transitions to IC Engine mode Driver warning provided</td>
</tr>
</tbody>
</table>
High Level System Element Hazard Analysis

- Fault Analysis Results

<table>
<thead>
<tr>
<th>HV / Motion Hazards</th>
<th>Detection</th>
<th>Mitigation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shock - High</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Burn - Medium</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Heat - High</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Acceleration - High</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Deceleration - Medium</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Direction - Medium</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Fault Analysis Results

<table>
<thead>
<tr>
<th>HV / Motion Hazards</th>
<th>Detection</th>
<th>Mitigation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shock - High</td>
<td>Voltage Sensors (Isolation)</td>
<td></td>
</tr>
<tr>
<td>Burn - Medium</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>Heat - High</td>
<td>Temp Sensors</td>
<td></td>
</tr>
<tr>
<td>Acceleration - High</td>
<td>Vehicle Speed, Clutch Speeds, Current Sensors, Torque Command Monitors</td>
<td></td>
</tr>
<tr>
<td>Deceleration - Medium</td>
<td>Vehicle Speed, Clutch Speeds, Current Sensors</td>
<td></td>
</tr>
<tr>
<td>Direction - Medium</td>
<td>Directional Speed Sensors, Torque Command Monitors</td>
<td></td>
</tr>
</tbody>
</table>
## Workshop Example Possible Answers

### Fault Analysis Results

<table>
<thead>
<tr>
<th>HV / Motion Hazards</th>
<th>Detection</th>
<th>Mitigation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shock - High</td>
<td>Current Sensors</td>
<td>Insulation, Physical Barriers, Protective Covers, Cable Routing, Driver Notification, Disconnect HV Battery</td>
</tr>
<tr>
<td>Burn - Medium</td>
<td>None</td>
<td>Prevention used to eliminate “hot spots” in design: Thermal Insulation / Isolation; Heat capacity of devices</td>
</tr>
<tr>
<td>Heat - High</td>
<td>Temp Sensors</td>
<td>Heat Shields, Protective Covers Disconnect HV Battery</td>
</tr>
<tr>
<td>Acceleration - High</td>
<td>Vehicle Speed, Clutch Speeds, Current Sensors, Torque Command Monitors</td>
<td>Disconnect HV Battery, Shutdown Motor Controller, Depower Motors</td>
</tr>
<tr>
<td>Deceleration - Medium</td>
<td>Vehicle Speed, Clutch Speeds, Current Sensors</td>
<td>Open Clutches, Shutdown Motor Controller, Depower Motors</td>
</tr>
<tr>
<td>Direction - Medium</td>
<td>Directional Speed Sensors, Torque Command Monitors</td>
<td>Override Torque Command, Open Clutches, Shutdown Motor Controller, Depower Motors</td>
</tr>
</tbody>
</table>
## Fault Analysis Results

<table>
<thead>
<tr>
<th>HV / Motion Hazards</th>
<th>Detection</th>
<th>Mitigation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shock - High</td>
<td>Current Sensors</td>
<td>Insulation, Physical Barriers, Protective Covers, Cable Routing, Driver Notification, <strong>Disconnect HV Battery</strong></td>
</tr>
<tr>
<td>Burn - Medium</td>
<td>None</td>
<td>Prevention used to eliminate “hot spots” in design: Thermal Insulation / Isolation; Heat capacity of devices</td>
</tr>
<tr>
<td>Heat - High</td>
<td>Temp Sensors</td>
<td>Heat Shields, Protective Covers <strong>Disconnect HV Battery</strong></td>
</tr>
<tr>
<td>Acceleration - High</td>
<td>Vehicle Speed, Clutch Speeds, Current Sensors, Torque Command Monitors</td>
<td><strong>Disconnect HV Battery</strong>, Shutdown Motor Controller, Depower Motors</td>
</tr>
<tr>
<td>Deceleration - Medium</td>
<td>Vehicle Speed, Clutch Speeds, Current Sensors</td>
<td>Open Clutches, Shutdown Motor Controller, Depower Motors</td>
</tr>
<tr>
<td>Direction - Medium</td>
<td>Directional Speed Sensors, Torque Command Monitors</td>
<td>Override Torque Command, Open Clutches, Shutdown Motor Controller, Depower Motors</td>
</tr>
</tbody>
</table>
System Control Structure

Driver

Vehicle Motion Desire

"Visceral" Vehicle Motion Feedback

IC Engine

IC Engine Torque to Driveline

Vehicle Motion

Power Coordination Communication

Engine Power Commands

Engine Feedback

Motor Control Module

Electric Motor Resolver Input

IC Engine

Torque to Driveline

Motor Control Module

Accel Pedal Sensor Input

Engine Control Module

3φ Motor Currents

Electric Motor Fdbk Back EMF Energy

Power Inverter Module

HV Supply Voltage

Recharge Voltage

HV Battery

HV Insulation and Isolation

Environmental Feedback Factors

Accelerator Pedal Assembly

Accelerator Pedal Assembly

Electric Machine and Inverter Feedback

Electric Machine and Inverter Feedback

Power Inverter Module

HV Insulation and Isolation

HV Insulation and Isolation

Electric Machines

Electric Motor Fdbk Back EMF Energy

Electric Power Commands

HV Supply Voltage

Recharge Voltage

HV Battery

HV Insulation and Isolation

HV Insulation and Isolation

Environmental Feedback Factors

Reproduction or Reuse of this Material is Prohibited without Express Permission from GM

ISSC 2015
Define System Requirements

➢ HV Requirements May Apply to Components
  ➢ Electrical Isolation
  ➢ Cable Routing Clearances and Radii
  ➢ Protective Covers
  ➢ Finger Proof Connectors
  ➢ Heat Shields
  ➢ Battery Voltage/Current Sensors

➢ Propulsion Requirements May Apply to Components
  ➢ Electric Machine Speed Sensors
  ➢ Electric Machine Current Sensors
  ➢ Vehicle Speed Sensors
  ➢ Controller Microprocessor Architecture
<table>
<thead>
<tr>
<th>Functional Group</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Propulsion Systems</td>
<td></td>
</tr>
<tr>
<td>Chassis Systems</td>
<td></td>
</tr>
<tr>
<td>Power Inverters</td>
<td></td>
</tr>
<tr>
<td>High Voltage Systems</td>
<td></td>
</tr>
<tr>
<td>Wire Harnesses</td>
<td></td>
</tr>
<tr>
<td>Sensors and Actuators</td>
<td></td>
</tr>
<tr>
<td>Software</td>
<td></td>
</tr>
</tbody>
</table>
## Identify and Inform Groups Needing System Requirements

<table>
<thead>
<tr>
<th>Functional Group</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Propulsion Systems</td>
<td>Output Shaft Speed Sensors, SW monitors</td>
</tr>
<tr>
<td>Chassis Systems</td>
<td>Electrical isolation</td>
</tr>
<tr>
<td>Power Inverters</td>
<td>Protective covers</td>
</tr>
<tr>
<td>High Voltage Systems</td>
<td>Finger proof connectors, electrical isolation, HV Battery Disconnect</td>
</tr>
<tr>
<td>Wire Harnesses</td>
<td>Cable routing clearances and bend radii</td>
</tr>
<tr>
<td>Sensors and Actuators</td>
<td>Sensing rates, resolution, response times</td>
</tr>
<tr>
<td>Software</td>
<td>Safety requirements integrity level (ASIL) Safety strategy and mitigation actions</td>
</tr>
</tbody>
</table>
Actual System Hardware and Software Design Activities

- Performance, Cost, Quality Trade-offs
- Component Packaging
- Design Reviews
- Budget Reviews
- DFMEAs, AFMEAs
- Simulation and Analysis
- Supplier Interactions
- Build 1st Prototype Unit
Test and Validate Prototype Hardware and Software

- Test components to verify requirements met
  - Hardware component tests
    - Environmental
    - Electrical
    - Mechanical
  - Software component tests
- Test subsystems and verify mitigation mechanisms
  - Electronic device bench testing
- Test vehicles and verify mitigation mechanisms
  - Define users and access
  - Perform initial development testing
- Update system design content as required
Test and Validate Production Hardware and Software

- Test component changes to verify requirements met
  - Hardware component tests (as required)
    - Environmental
    - Electrical
    - Mechanical
  - Software component tests (as required)

- Test subsystems and verify mitigation mechanisms
  - Electronic device bench testing
  - Test and validate safety diagnostics
  - Evaluate mitigation action performance

- Test vehicles and verify mitigation mechanisms
  - Update users and access
  - Continue development testing

- Update system design content as required
Perform Final Vehicle Safety Testing

- Verification confirms that work products properly reflect the requirements specified for them ("you built it right")
  - Methods used for Verification are: Analysis (e.g. FTA, FMEA), Demonstration, Inspection and Testing

- Validation confirms that the product fulfills its intended use in all of the environments that the product will be used in ("you built the right thing")
  - During Safety validation, e.g. hazard testing is performed to confirm that the hazard metrics are satisfied

- Complete Vehicle Level Safety Conformance Evaluation
Document Safety Validation Results

- Traceability to Requirements
  - Source of Requirement
  - HW and SW Content Technical Specifications
  - V&V Test Procedures

- Objective Evidence
  - Safety Reviews
  - V&V Test Result Summaries

- Final Safety Assessment
  - Approvals
  - Documentation
  - Archive and Retention
Tutorial Summary

- System Safety is a disciplined and comprehensive engineering effort to identify safety related risks to be either eliminated or controlled.

- System Safety assessments early in the process are essential.

- A robust safety process is key and management support to employ and enforce it is critical.

- Clear, well defined requirements are necessary.

- Validation and verification are critical for success.
Questions and Answer Period
Thank You
Definition for Hazard Severity

<table>
<thead>
<tr>
<th>Hazard Severity</th>
<th>Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>S0*</td>
<td>Low</td>
<td>No injuries</td>
</tr>
<tr>
<td>S1</td>
<td>Moderate</td>
<td>Light or moderate non life-threatening injuries to the driver or passengers or people around the vehicle</td>
</tr>
<tr>
<td>S2</td>
<td>Serious</td>
<td>Severe and life-threatening (Survival possible) to the driver or passengers or people around the vehicle or in other surrounding vehicles</td>
</tr>
<tr>
<td>S3</td>
<td>Severe</td>
<td>Life-threatening injuries (Survival uncertain, fatal injuries) to the driver or passengers or people around the vehicle or in other surrounding vehicles</td>
</tr>
</tbody>
</table>

Note: *No ASIL is assigned for S0

In evaluating the severity component of risk for a hazard, always work with the WORST CREDIBLE consequence.

Source ISO 26262
Workshop Tutorials

Risk = function of (S, E, C) = (Severity, Exposure, Controllability)

### Definition for Likelihood of Exposure to Vehicle Operating Scenarios

<table>
<thead>
<tr>
<th>Exposure</th>
<th>Title</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>E0*</td>
<td>Incredible</td>
<td>Situations that are extremely unusual.</td>
</tr>
<tr>
<td>E1</td>
<td>Rare</td>
<td>Very low probability. Situations that occur less often than once a year for the great majority of drivers</td>
</tr>
<tr>
<td>E2</td>
<td>Sometimes</td>
<td>Low probability. Situations that occur a few times a year for the great majority of drivers. &lt; 1% of average operating time</td>
</tr>
<tr>
<td>E3</td>
<td>Quite often</td>
<td>Medium probability. Situations that occur once a month or more often for an average driver. 1% - 10% of average operating time.</td>
</tr>
<tr>
<td>E4</td>
<td>Often-Always</td>
<td>High probability. All situations that occur during almost every drive on average. &gt; 10% of average operating time.</td>
</tr>
</tbody>
</table>

Note: *No ASIL is assigned for E0*  

Source ISO 26262
Definition for Controllability

<table>
<thead>
<tr>
<th>Vehicle Controllability</th>
<th>Title</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>C0*</td>
<td>Controllable in general</td>
<td>Generally Controllable by all drivers;</td>
</tr>
<tr>
<td>C1</td>
<td>Simply Controllable</td>
<td>Less than 1% of average drivers or other traffic participants are usually unable to control the damage. In this kind of a hazard scenario, it is likely that the vehicle will be controllable by most drivers. Again controllable is used in the sense that most drivers will be able to prevent a mishap by applying corrective counter steering/ or corrective braking.</td>
</tr>
<tr>
<td>C2</td>
<td>Normally Controllable</td>
<td>Less than 10% of average drivers or other traffic participants are usually unable to control the damage. In this kind of a hazard scenario, it is possible that the vehicle will be controllable by some drivers. Again controllable is used in the sense that some drivers will be able to prevent a mishap by applying corrective counter steering/ or corrective braking.</td>
</tr>
<tr>
<td>C3</td>
<td>Difficult to Control</td>
<td>The average driver or other traffic participant is usually unable, or barely able, to control the damage. In this kind of a hazard scenario, it is unlikely that the vehicle will be controllable by average driver. Again uncontrollable is used in the sense that the average driver will be unable to prevent a mishap by applying corrective counter steering/ or corrective braking</td>
</tr>
</tbody>
</table>

Note: *No ASIL is assigned for C0

Source ISO 26262

Risk = function of (S, E, C) = (Severity, Exposure, Controllability)