System Safety Process Applied to An Automotive High Voltage Propulsion System

Mark Vernacchia
GM Technical Fellow
Principal System Safety Engineer – Propulsion Systems

Galen Ressler
GM Technical Fellow
Principal System Safety Engineer – High Voltage Systems
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 How to Translate Hazards to Requirements
- Understanding of What is a “good” Requirement
- Understanding of the Process Applied to Develop Requirements
- 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
  - High Voltage 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.
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.
System Safety Process Overview

- A system safety process following 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
- Preliminary Hazard Analysis
- System Safety Program Planning
- System Safety Concept
- Single Element Fault Analysis
- Safety Concept Review

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

Concept Changes

Design
- 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

Requirements Changes

Development / Implementation
- Software Fault Tree Analysis
- Software Detailed FMEA
- Software Code Reviews
- Closure of FTA / FMEA Issues
- Safety Implementation Review
(Separate or Combined with Production Safety Design & Test Review)

Design Changes

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

Design Corrections

Production / Deployment
- Production Observed Design Discrepancies

Safety Analysis Tasks

Production Observed Design Discrepancies

Concept

Requirements

Design

Development / Implementation

Verification & Validation

Production / Deployment
System Safety Process Typical Phases

- A 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
Began System Safety Strategy Determination

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

Deliverables (typical): PHA and/or HARA, SEHA, Program Schedule (w/ milestones), Overall Summary Document (Hazards, Risk Rating, Detection Strategy, Mitigation Strategies)
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 Maneuver
- 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
High Level Functional Definition of the Feature/System

- Define the System/Feature
- List and define the vehicle level functions (driver interface, vehicle output: block diagram)
- Define the system scope and boundary (high level block diagram including the driver/operator, vehicle output)
- Understand the function under intended operating conditions
  - Understand potential interactions with other functions in the vehicle
  - Identify mechanisms for energy release from the system – energy outlets
    - Consider the various actuators that the system controls or influences
  - What parameter(s) of the vehicle does the system output influence
    - Longitudinal, Lateral, Angular moments etc.
  - Employ systems thinking – Holistically
- Consider service, maintenance and disposal phases too
  - Life cycle of the system
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
Safety Analysis Techniques

- Several different types of analysis may be employed to examine the design from different perspectives

- Deductive analysis - An analysis technique that starts with a single consequence and explores all the possible causes that can lead to the consequence.
  - The Software Fault Tree Analysis (FTA) described here is an example of deductive analysis

- Inductive analysis - An analysis technique that starts with a single cause and explores all the possible consequences.
  - The detailed Software Failure Modes and Effects Analysis (FMEA) described here is an example inductive analysis

- Exploratory analysis - An analysis technique which starts with a deviation and explores all the possible consequences and causes (if possible) for that deviation.
  - Hazard and Operability Analysis (HAZOP) is an example of exploratory analysis. HAZOP typically involves the use of “Guidewords” to direct the analysis. Software System FMEA described here is an example of HAZOP analysis.
System Analysis: Causes vs. Effects

<table>
<thead>
<tr>
<th>Effects</th>
<th>Unknown</th>
<th>Known</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unknown</td>
<td><strong>Exploratory Analysis</strong></td>
<td><strong>Inductive Analysis</strong></td>
</tr>
<tr>
<td>Known</td>
<td><strong>Deductive Analysis</strong></td>
<td><strong>Descriptive Analysis</strong></td>
</tr>
</tbody>
</table>

- Deductive Analysis (example: FTA)
- Inductive Analysis (examples: FMEA, Interface Analysis, Sneak Circuit Analysis)
- Exploratory Analysis (HAZOP, what-if)
- Descriptive Analysis – relatively straight forward observations
System Analysis: Causes vs. Effects

**FMEA**
Start with the known causes

Inductive Reasoning

Possible effects

**FTA**
Possible causes

Deductive Reasoning

Start with the known Effects

**HAZOP**
Possible causes

Exploratory Reasoning

Start with single deviation

Exploratory Reasoning

Possible effects
Perform System Level 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
Human Machine Interaction- Systems Thinking

Picture source: http://www.sms.hest.ethz.ch/mission
Generic Control Structure

- **Operator**
- **Input Controls**
- **Computer/Human Control**
- **Actuators**
- **Controlled Process in the Vehicle**
- **Operator Feedback**
- **Feedback**

*Actuator control can be manual and/or electrical/electronic based

**Feedback can be tactile/perceptible and/or electrical/electronic based
Interface vs Interaction

- **Interface**
  - When there is some kind of direct data/info transfer and/or communication between two systems or system elements within a system

- **Interaction**
  - When a system state affects or influences one or more vehicle systems, or system elements, even if they may not be connected or communicating with each other
    - Impact may be due to physics, vehicle design/configuration, and/or architectural design dependencies
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, Too Much, Too Little
  - Frozen/Stuck
  - Different Direction / Polarity

- 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.
## Identifying Hazards: HAZOP Guidewords

<table>
<thead>
<tr>
<th>System Function Vs. Guidewords</th>
<th>Not Provided</th>
<th>Provided Leads to Unsafe Condition</th>
<th>Incorrect Function (Less than requested)</th>
<th>Incorrect Function (Wrong direction)</th>
<th>Unintended Activation (Incorrect Timing)</th>
<th>Locked/Stuck Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Electric Steering Assist Function</td>
<td>Loss of Steering Assist</td>
<td>Excessive Steering Assist</td>
<td>Reduced Steering Assist</td>
<td>Steering in the opposite direction (reverse steering)</td>
<td>Unintended Steering</td>
<td>Locked Steering</td>
</tr>
<tr>
<td>Base brake function</td>
<td>Loss of Brakes</td>
<td>Excessive Brake Apply</td>
<td>Reduced Brake apply</td>
<td>-</td>
<td>Unintended Brake Apply</td>
<td>Stuck Brakes</td>
</tr>
<tr>
<td>Electronic Stability Control (ESC)</td>
<td>Loss of ESC</td>
<td>Excessive Yaw Moment Correction</td>
<td>Inadequate Yaw Moment Correction</td>
<td>Incorrect Yaw moment Correction</td>
<td>Unintended ESC Apply</td>
<td>Stuck ESC</td>
</tr>
</tbody>
</table>
## High Level System Element Hazard Analysis

### Summary Table

<table>
<thead>
<tr>
<th>Function</th>
<th>Unsafe Actions (Guidewords)</th>
<th>Causes</th>
<th>Constraints (Requirements)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Provide Electric Motor Speed</strong></td>
<td>Unknown motor speed</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Incorrect motor speed</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Indicates motor spinning in opposite direction</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Speed provided too late/early for receiving module to read</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Frozen motor speed</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Summary Table

<table>
<thead>
<tr>
<th>Function</th>
<th>Unsafe Actions (Guidewords)</th>
<th>Causes</th>
<th>Constraints (Requirements)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provide Electric Motor Speed</td>
<td>Unknown motor speed</td>
<td>Broken Wire</td>
<td>Run sensor diagnostics</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Failed Sensor</td>
<td>Run sensor diagnostics</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Loose Connector</td>
<td>Run sensor diagnostics</td>
</tr>
<tr>
<td></td>
<td>Incorrect motor speed</td>
<td>Faulty Sensor</td>
<td>Run comparison with vehicle speed info</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Corrupted Message</td>
<td>Add Alive Rolling Counts and Check Sums</td>
</tr>
</tbody>
</table>
System Engineering “V” Model with Safety Phases

Hazard Metric Translation

- Hazard metrics are translated into engineering requirements
  - The intent of this system safety task is to translate the Vehicle Level Hazard metric to the system safety engineering requirement. The applicable vehicle level hazard metrics, based on the PHA report, are used in deriving system specific safety requirements.

  1. **Vehicle Level Hazard Metric**

  2. **Translate into system engineering requirements by analysis or test**

  3. **Confirm that the translated engineering requirements are correct for the target vehicle**

- **If vehicle is not available, use approximate actuator response times, and vehicle dynamics to estimate conservatively**

- **When test vehicle or accurate vehicle data becomes available confirm in simulation or in actual vehicle by test**
Highest System Safety Requirement:
The propulsion system shall not cause an unintended acceleration that can exceed 0.15g - 0.25g within 150 ms - 200 ms

Hazard Metric Translation Process

System Safety Requirements document

(Example)
1500 Nm of Motor Torque within 200 ms.

Hybrid Torque Safety SSTS document

The worst case remedial action time is 200ms for all relevant safety checks and diagnostics.
Hazard Metric Translation Example

The translation is made using the Law of Motion to convert the theoretical force (N) required to accelerate the vehicle (and exceed the unintended acceleration metric) into an engine crankshaft torque (Nm).

Starting with \( F = \text{Mass} \times \text{Acceleration} \)

where \( F = \text{The force acting on the vehicle that will cause, for example, } 0.2\text{g acceleration} \)

\( M = \text{Vehicle Mass (Curb Weight)} = X \text{ (kg)} \)

\( A = \text{Unintended acceleration} = 0.2\text{g} \)

\( F = X \text{ (kg)} \times (0.2) \times (9.812\text{m/s}^2) = Y \text{ (N)} \)

Axle Torque = Tire Radius \times Force

Tire Radius = Z \text{ (m)}

Axle Torque = Z \text{ (m)} \times Y \text{ (N)} = W \text{ (Nm)}

Output Torque (Transmission) = Axle Torque / Final Drive Ratio

Final Drive Ratio = R

Output Torque (Transmission) = W \text{ (Nm)} / R = Q \text{ (Nm)}

Crankshaft Torque = Q \text{ (Nm)} / (G \times 1.0) = T \text{ (Nm)}

Transmission Gear Ratio (1\text{st} Gear) = G
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
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

➢ How to Start . . . ??
Functional Interface Analysis: Overview

- Functional System Interface Analysis identifies critical interactions within the system
  - The intent of this analysis task is to understand the functional interfaces and the possible functional interactions in the system between different subsystems and system elements, which can include sensors, controllers, and actuators

- System functional hazard analysis involves the process of analyzing the potential functional behavior of the system

- All possible functional interactions with other vehicle systems are considered and analyzed for possible conflicts that can have potential safety implications

- This process enables identification of the safety critical interactions and thus the safety critical interfaces
Vehicle Level System/Feature Interaction

- Safety critical systems have at least two functional states (ON, OFF)
  - Some of the states may be considered a safe state when viewed from that system or feature standpoint
    - i.e., when viewed in isolation
  - However a safe state for one system/feature does not necessarily mean it is a safe state for the other - because of interaction
  - Interaction can be vehicle dynamics/physics/architectural choice

- Examples:
  - Locking of active rear steer requires the steering wheel angle to have an offset to drive the vehicle straight
    - By itself, locked ARS is a safe state.
    - But not when the vehicle has other features such as ESC/ CMB/ FSRACC etc.
    - Correlation between yaw, lateral acceleration
    - SWA is disturbed - vehicle heading angle disturbed
  - ETRS dependency on EPB. Loss of Park engage is a safe state for EPB, but not with ETRS. EPB is a fall back option for ETRS – by design choice
  - Feature/system dependencies on power moding
    - Feature turns off when power mode changes, but vehicle continues moving
Functional Interface Analysis Methodology

- The major guide words that are considered (as applicable) in the HAZOP (what-if) analysis of the system functional interfaces include:
  1. Loss of data (includes communication loss or loss of source itself)
  2. Interrupted communication (Incomplete data)
  3. Transmission of corrupted/incorrect data
  4. Aged data (if applicable)

- This analysis process should also consider the potential for interactions of functions between subsystems.
  - For example, the engine control and the brake control may be both be activated at the same time correctly by two different functionalities trying to achieve their intended function, but the overall result at the vehicle may be undesirable and potentially may have safety implications.
Functional Interface Analysis Methodology

This analysis process involves the evaluation of:

1. System functional behavior and its interactions with other systems in the vehicle including the user/operator if applicable

2. Functional interactions between different subsystems or control modules within the system. This applies to a distributed system

3. Functional interactions between sensors inputs and system actuator outputs

4. Analyze **possible conflicting interacting or competing interactions** between system functions or and/or features that can have system safety implications

Hazard Operability Analysis technique can be applied to evaluate the functional interfaces between subsystems and component.

I. HAZOP guidewords is applied to every input and output of subsystems/components to understand the potential safety implications.

II. In addition, the communication medium itself is also analyzed.
Derive Functional Safety Requirements

To derive Functional Safety requirements, develop a strategy to satisfy the safety goals identified in the PHA:

- For each hazard explain high level strategy and derive vehicle level safety requirements based on hazard metrics (if available) and the ASIL
  - Functional safety requirements must be design agnostic (thus re-usable)

- Apply systems theory principles and derive functional integrity requirements for the various control elements.

- The generic control structure provides a reference guide to consider the various elements that can be part of the functional system.
  - Note: The control structure is not necessarily the system design. Safety is a system property and a controls problem. Hence to derive functional safety requirements it is essential to model the functional control structure to understand the functional control flow and thus derive the safety requirements and constraints that the control elements contribute.

- For each contributing element in the functional control flow, specify safety constraints in terms of integrity requirements for the element
What are Effective Requirements?

- **Effective Requirements...**
  - are written with correct grammar
  - meet quality criteria
  - contain the correct content for their type
  - are written at the correct level of abstraction
Good Requirement Criteria

- Requirement – A statement of what is wanted or what is to be accomplished

- All Requirements use the verb “SHALL”.

- Requirement Quality Criteria:
  - Atomic – Cannot be split into further requirements
  - Complete – Includes: subject, action, object (if applicable), conditions, requirement verb, and negotiated value
  - Unambiguous – All parties can agree on what it means
  - Feasible – Can be implemented within constraints of project
  - Verifiable – There is a way to test the system meets the requirement
Requirement Grammar

- Subject (Actor)
- Requirement Verb ("shall")
- Action/Object
- Negotiated Value
- Conditions

**Example:**

“The class shall provide a round of applause to the instructor lasting at least 4 seconds after reading this example.”
Requirement Grammar

- **Subject (Actor)**
- **Requirement Verb ("shall")**
- **Action/Object**
- **Negotiated value**
- **Conditions**

**Example:**

"The class shall *provide a round of applause to the instructor lasting at least 4 seconds after reading this example.*"
The Requirement Grammar

The Requirement Verb is “shall”

Unacceptable verbs include:

- Must
- Will
- Should
- Could
- Can
- May

Example:
“The Forward Lighting Feature must allow the driver to see the road at night.”

Better Requirement Verb:
“The Forward Lighting Feature shall allow the driver to see the road at night.”
Requirement Grammar

➢ Action/Object
  ➢ The Action is the transitive verb that the subject is performing
  ➢ The Direct Object is the recipient of the action
  ➢ An Indirect Object is the recipient of the Direct Object (not always necessary)

Example:
“The Forward Lighting Feature shall allow the driver to see the road at night.”

Better Action/Object:
“The Forward Lighting Feature shall illuminate the vehicle’s forward path at night.”
Negotiated Value

The extent to which the action shall be performed

- Single limit boundary (e.g., a maximum value)
- Range of values (between two boundaries)
- Nominal value (within tolerances)

Example:

“The Forward Lighting Feature shall illuminate the vehicle’s forward path at night.”

Better Negotiated Value:

“The Forward Lighting Feature shall illuminate the vehicle’s forward path with 100 to 200 lux at 10m at night.”
Requirement Grammar

- Conditions
  - The circumstances under which the negotiated value shall be met
    - Ambient environmental conditions
    - The state of the Feature/System
    - Vehicle configurations (interfacing Feature/System is available)
    - Feature/System variants

**Example:**

“The Forward Lighting Feature shall illuminate the vehicle’s forward path with 100 to 200 lux at 10m at night.”

**Better Conditions:**

“The Forward Lighting Feature shall illuminate the vehicle’s forward path with 100 to 200 lux at 10m **when the Feature is in the Low Beam state.**”
<table>
<thead>
<tr>
<th>Subject</th>
<th>Requirement Verb</th>
<th>Action / Object</th>
<th>Negotiated Value</th>
<th>Conditions</th>
</tr>
</thead>
<tbody>
<tr>
<td>The class</td>
<td>shall</td>
<td>provide a round of applause to the instructor</td>
<td>lasting at least 4 seconds</td>
<td>after reading this example.</td>
</tr>
<tr>
<td>The Forward Lighting Feature</td>
<td>shall</td>
<td>illuminate the vehicle’s forward path</td>
<td>with 100-200 lux @10m</td>
<td>when the Feature is in the Low Beam state.</td>
</tr>
</tbody>
</table>
Requirement Grammar

- Subject (Actor)
- Requirement Verb ("shall")
- Action/Object
- Negotiated value
- Conditions

Example:

“When the door is opened, a 60 dBA chime shall be provided to the driver by the Audible Alert System if the keys are in the ignition.”
Requirement Grammar

- Subject (Actor)
- Requirement Verb (“shall”)
- Action/Object
- Negotiated value
- Conditions

Example:
“When the door is opened, a 60 dBA chime shall be provided to the driver by the Audible Alert System if the keys are in the ignition.”

Better Example:
“The Audible Alert System shall provide a chime to the driver of 60 dBA when the door is opened and the keys are in the ignition.”
Requirement Summary and Allocation

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

System Safety Requirements

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

- Physical Subsystem
  - Housing Cells
  - Electrical Electronics Module
  - Physical Components
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
- How to Start . . . ??
The next step is to decompose and allocate the requirements to hardware and software components. The goal is to define software and hardware functional requirements that comprehend the identified system and subsystem safety requirements.

Once the safety requirements are identified, they are verified for correctness, clarity, completeness, and consistency through informal reviews with the appropriate technical experts and all the stakeholders for the project. Conflicting requirements are resolved.

The traceability of system/subsystem safety requirement to lower level hardware and software component functional requirements is preserved as part of the requirements management process.
Traceability Simplified

Hazard

Requirement 1 • Test Case

Requirement 2 • Test Case

Requirement 3 • Test Case
Example of Traceability

Legend: The ovals represent the specific technical item within a work-product. The text in red outside the oval represents the work product where it is captured in the GM System Safety Process.
### Traceability Matrix

<table>
<thead>
<tr>
<th>ID</th>
<th>System Safety Requirement</th>
<th>Source Traceability (Origin of the Safety Requirements)</th>
<th>Allocation Traceability (Create additional columns if needed to show detailed traceability)</th>
<th>Traceability To V&amp;V Plans and Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABC_SS R_009</td>
<td>The ABC sensor 1 Diagnostics shall meet the following criteria: Open, Short, Stuck in range, Out-of-Range, and Offset within range (resistive short)</td>
<td>PHA</td>
<td>Sensor #1</td>
<td>Test 3</td>
</tr>
<tr>
<td>ABC_SS R_003</td>
<td>The Steering Subsystem shall compute signal A satifing high integrity</td>
<td>Hazard #5</td>
<td>Steering System</td>
<td>Test 2</td>
</tr>
<tr>
<td>ABC_SS R_001</td>
<td>The system shall not violate the hazard metric for hazard #01.</td>
<td>PHA Hazard # 1</td>
<td>DFMEA</td>
<td>Test 3</td>
</tr>
</tbody>
</table>

- Be sure to track where each requirement is originated from. This can be more than one source
- Also it can be allocated to multiple areas and require different tests
- Capture everything
Specification – Collection of Requirements

Specifications should be traceable

All Requirements can be traced back to their source. (person or requirement it was derived from)

Specifications need to be checked for redundancy
Validation & Verification Traceability

- High level safety V&V plans must be available for the safety requirements review
- Involve validation teams to develop that initial plan
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 for expected vehicle performance is helpful
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 1<sup>st</sup> 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\textsuperscript{st} 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

System Safety Requirements

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

Physical Subsystem
- Housing Cells
- Electrical Electronics Module
- Physical Components

Safety Goals Achieved

System Validation

Functional Subsystem Verification

Physical Subsystem Verification

Safety Goals Achieved
Create Safety Case

- A Safety Case is a document that provides convincing and valid assertions 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
System Content – Safety Critical Areas

- Accelerator Pedal Assembly
- 12V Battery
- Engine Control Module
- Electric Machines
- Engine
- HV Battery
- Power Inverter Module
- Motor Control Module
- 12V Battery
- Engine
- HV Battery
- Power Inverter Module
- Motor Control Module
- Electric Machines
System Control Structure

Vehicle Motion Desire

Driver

"Visceral" Vehicle Motion Feedback

Vehicle Motion

Environmental Feedback Factors

Accelerator Pedal Assembly

Engine Control Module

Power Inverter Module

Motor Control Module

Power Coordination Communication

Electric Motor Resolver Input

Power Inverter Module

Electric Motor and Inverter Feedback

Engine Power Commands

Engine Feedback

Electric Motor Fdbk

Back EMF Energy

HV Supply Voltage

HV Insulation and Isolation

3Φ Motor Currents

Recharge Voltage

IC Engine

HV Battery

IC Engine Torque to Driveline

Electric Torque to Driveline

Power Coordination Communication

Environmental Feedback Factors

Field Control Module
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

<table>
<thead>
<tr>
<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>
</tr>
</tbody>
</table>

### Exposure

<table>
<thead>
<tr>
<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>
</tr>
</tbody>
</table>

### Controllability

<table>
<thead>
<tr>
<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>
</tr>
</tbody>
</table>
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
System Control Structure

- **Driver:**
  - Vehicle Motion Desire
  - "Visceral" Vehicle Motion Feedback

- **Engine Control Module:**
  - Engine Power Commands
  - Engine Feedback
  - Power Coordination Communication

- **IC Engine:**
  - IC Engine Torque to Driveline

- **Electric Machines:**
  - Electric Torque to Driveline
  - 3Φ Motor Currents
  - Electric Motor Fdbk Back EMF Energy

- **Power Inverter Module:**
  - HV Supply Voltage
  - Recharge Voltage

- **Electric Machine and Inverter Feedback:**
  - Electric Power Commands

- **Motor Control Module:**
  - Electric Motor Resolver Input

- **Accelerator Pedal Assembly:**
  - Accel Pedal Sensor Input
# 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>
## High Level System Element Hazard Analysis

<table>
<thead>
<tr>
<th>Primary Fault</th>
<th>Resulting Fault</th>
<th>Accelerator Pedal Assembly</th>
<th>12V Battery Power</th>
<th>Engine Control Module</th>
<th>Motor Control Module</th>
<th>Electric Machine</th>
<th>Electric Motor Resolver</th>
<th>Power Inverter</th>
<th>Battery Disconnect</th>
<th>HV Battery</th>
<th>HV Insulation</th>
<th>CAN</th>
<th>Resulting State</th>
<th>Safety Hazard Present?</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;0&quot; = Not Operating</td>
<td>0</td>
<td>Primary Fault</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>System Working Properly</td>
<td>No</td>
</tr>
<tr>
<td>&quot;0&quot; = Not Operating</td>
<td>0</td>
<td>Resulting Fault</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>Accel Pedal Assembly Fails</td>
<td>HIGH</td>
</tr>
<tr>
<td>&quot;0&quot; = Not Operating</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>All controllers fail &lt;OFF&gt;</td>
<td>LOW</td>
<td></td>
</tr>
<tr>
<td>&quot;1&quot; = Operating Normally</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>ECM Fails &lt;OFF&gt;</td>
<td>LOW</td>
<td></td>
</tr>
<tr>
<td>&quot;1&quot; = Operating Normally</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>IC Engine Shutdown</td>
<td>LOW</td>
<td></td>
</tr>
<tr>
<td>&quot;1&quot; = Operating Normally</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>MCM Fails &lt;OFF&gt;</td>
<td>LOW</td>
<td></td>
</tr>
<tr>
<td>&quot;1&quot; = Operating Normally</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>Electric Motor Shutdown</td>
<td>LOW</td>
<td></td>
</tr>
</tbody>
</table>

**Safety Hazard Present?**

- **High**: Unintended Longitudinal Motion
- **Low**: Loss of Propulsion

**Notes:**
- "0" = Not Operating
- "1" = Operating Normally
- "1" = Operating Normally
# 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>No</td>
<td>NA</td>
<td>ECM commands IC engine shutdown and vehicle transitions to a non-propulsion state.</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>Propulsion Shutdown</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>Propulsion Shutdown</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>EV mode</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>EV mode</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>IC Engine Mode</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>IC Engine Mode</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></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>Current Sensors</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>
## 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>
## 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>
System Control Structure

Driver

Vehicle Motion Desire

Engine Control Module

Accel Pedal Sensor Input

Power Coordination Communication

Electric Motor Resolver Input

3Φ Motor Currents

Electric Motor Feedback

Back EMF Energy

Electric Machines

Engine

Engine Power Commands

Engine Feedback

IC Engine

IC Engine Torque to Driveline

Vehicle Motion

Vehicle Motion Feedback

"Visceral" Vehicle Motion Feedback

Motor Control Module

Electric Machine and Inverter Feedback

Power Inverter Module

HV Supply Voltage

HV Insulation and Isolation

HV Battery

Recharge Voltage

Environmental Feedback Factors

Accelerator Pedal Assembly

Ambient Conditions

Power Coordination Communication

Electric Power Commands

Electric Motor Feedback

Back EMF Energy

Electric Machines

Electric Torque to Driveline

HV Insulation and Isolation

HV Insulation and Isolation

HV Battery

Recharge Voltage

Environmental Feedback Factors
System Control Structure

- Accelerator Pedal Assembly
- Engine Control Module
- Motor Control Module
- Power Inverter Module
- Electric Machines
- Electric Power Commands
- Electric Motor Resolver Input
- 3Φ Motor Currents
- Electric Motor Feedback
- Back EMF Energy
- HV Supply Voltage
- Recharge Voltage
- HV Battery

Driver:
- Vehicle Motion Desire
- "Visceral" Vehicle Motion Feedback

IC Engine:
- Engine Power Commands
- Engine Feedback
- IC Engine Torque to Driveline

Vehicle Motion:
- Electric Torque to Driveline

Environmental Feedback Factors

Power Coordination Communication:
- Accel Pedal Sensor Input
- Electric Machine and Inverter Feedback

HV Insulation and Isolation

ADDED Battery Disconnect
## Summary Table

<table>
<thead>
<tr>
<th>Function</th>
<th>Unsafe Actions (Guidewords)</th>
<th>Causes</th>
<th>Constraints (Requirements)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Provide Electric Motor Speed</strong></td>
<td>Unknown motor speed</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Incorrect motor speed</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Summary Table

<table>
<thead>
<tr>
<th>Function</th>
<th>Unsafe Actions (Guidewords)</th>
<th>Causes</th>
<th>Constraints (Requirements)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provide Electric Motor Speed</td>
<td>Unknown motor speed</td>
<td>Broken Wire</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Failed Sensor</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Loose Connector</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Incorrect motor speed</td>
<td>Faulty Sensor</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Corrupted Message</td>
<td></td>
</tr>
</tbody>
</table>
## High Level System Element Hazard Analysis

### Summary Table

<table>
<thead>
<tr>
<th>Function</th>
<th>Unsafe Actions (Guidewords)</th>
<th>Causes</th>
<th>Constraints (Requirements)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provide Electric Motor Speed</td>
<td>Unknown motor speed</td>
<td>Broken Wire</td>
<td>Run sensor diagnostics</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Failed Sensor</td>
<td>Run sensor diagnostics</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Loose Connector</td>
<td>Run sensor diagnostics</td>
</tr>
<tr>
<td></td>
<td>Incorrect motor speed</td>
<td>Faulty Sensor</td>
<td>Run comparison with vehicle speed info</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Corrupted Message</td>
<td>Add Alive Rolling Counts and Check Sums</td>
</tr>
</tbody>
</table>
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
## 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></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>
<tr>
<td>Functional Group</td>
<td>Requirements</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-------------------------------------------------------------------</td>
</tr>
<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)</td>
</tr>
<tr>
<td></td>
<td>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 1\textsuperscript{st} 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 ??????
Thank You