Drive Control Unit Requirements

for electric drive system

Requirements & Best Practice

draft 010

1863 Service Court, Riverside CA
92507

Note: The requirements in this document are for additional protocol only and is not a complete reference of the systems operation.

Originated from VCU requirements from Gtake drives on previous ZEPS vehicles.

Change log

01	Original
02	Implemented suggested improvements to form a readable document in word
03	Bare minimum USING STANDARD REQUIREMENTS
04	Updates and corrections to 03
05	Addition of hardwire throttle interlock
06	Application of iterative AI corrections
07	Changed throttle requirements to meet standards. Removed hardwire disconnect.
08	Edit / review version
09	Modified section 4
10	Modified section 8

Vehicle Control Unit (VCU) System Requirements

Compliant Design conforming to component standards

Document Version: 010 DRAFT
Date: 2025-11-3

Reference Documents:

The following reference documents are to be determined by other integration systems.

- VCU CAN Protocol Specification (Spreadsheet)
- Fault code table

Other reference documents:

- HARA

Library of Terms

Acronyms/Abbreviations:

- **VCU** - Vehicle Control Unit
- **BMS** - Battery Management System
- **CAN** - Controller Area Network
- **MIL** - Malfunction Indicator Light
- **RPM** - Rotations per minute of the drive motors
- **HVIL** - High Voltage Interlock
- **ASIL** - Automotive Safety Integrity Level
- **DCL** - Discharge Current Limit
- **CCL** - Charge Current Limit
- **TPS** - Throttle Position Sensor
- **ADC** - Analog-to-Digital Converter
- **EEPROM** - Electrically Erasable Programmable Read-Only Memory
- **RAM** - Random Access Memory
- **ROM** - Read-Only Memory
- **DTC** - Diagnostic Trouble Code
- **CRC** - Cyclic Redundancy Check
- **FMVSS** - Federal Motor Vehicle Safety Standards
- **UN-R** - United Nations Regulation
- **SAE** - Society of Automotive Engineers
- **ISO** - International Organization for Standardization
- **ABS** - Anti-lock Braking System
- **WCET** - Worst Case Execution Time
- **MAC** – Message Authentication code

Technical Terms:

- **Precharge** - Process of gradually charging high-voltage capacitors to match battery voltage before closing main contactor
- **Contactor** - High-voltage relay that connects/disconnects battery from drive system
- **Torque Request** - Commanded motor torque output as percentage (0-100%)
- **Deadband** - Minimum throttle position below which no torque is commanded
- **Limp Mode** - Reduced performance operating mode allowing vehicle movement despite faults
- **Turtle Mode** - Reduced performance mode.
- **Hill Hold** - System that maintains brake pressure when stopped on incline
- **Regen/Regenerative Braking** - Converting vehicle kinetic energy back to electrical energy during deceleration

Vehicle-Specific Terms:

- **ZEPS** – Zero Emission Propulsion System

Safety/State Terms:

- **READY State** - Normal operating state where drive system is functional
- **FAULT State** - Degraded state with automatic recovery attempts
- **EMERGENCY_STOP State** - Critical fault state requiring manual reset
- **Rollaway** - Unintended vehicle movement when in neutral without brakes

1. SYSTEM OVERVIEW

1.1 Purpose

REQ-001 [ASIL-D]

The Vehicle Control Unit (VCU) is the central controller for electric vehicle drive functions, responsible for:

- Throttle input processing and torque command generation
- Safety interlocks and fault management
- Battery current limit compliance (DCL/CCL)
- Auxiliary system control (fans, pumps, precharge, hill hold)
- CAN bus communication with motor controller and BMS

1.2 Intent

The design requirements used in this document are guided by the following standards:

Safety Requirement	Standard(s)	Notes
Prevention of unintended acceleration	FMVSS No. 124, ISO 26262	FMVSS 124 for brake override; ISO 26262 for fault detection/response
Brake pedal override priority	FMVSS No. 124, UN-R13-H Annex 4 (UNECE)	Choose based on your target market
Fault handling for throttle sensors	ISO 26262 Part 9	ASIL-dependent requirements for redundancy
Safe state transitions on fault detection	ISO 26262 Part 6 (Software)	State machine safety requirements
Throttle sensor voltage ranges & correlation	SAE J1843	Only if specifying pedal hardware (not VCU logic)
Torque tracking/plausibility checks	ISO 26262	Freedom from interference, systematic capability
Watchdog/supervision requirements	ISO 26262 Part 5 (Hardware) & Part 6 (Software)	-
CAN communication fault handling	ISO 26262 Part 6	Communication safety requirements
Brake condition warning	FMVSS 105, 135	Hydraulic and electric braking systems
Safe Gear Engagement	FMVSS 102, 114	Unsafe shift and unintended motion

1.2.1 The intent of this document is to guide the development of a safe, effective VCU. There should be no assumption that every part of this document must be adhered to, and no assumption that every requirement is contained therein. At any time, these requirements can change.

1.3 Design Process

- Complete these requirements.
- Use a development platform to frame and test code
- Design and build a custom device ($400 to $800 each for the completed part)
- Develop Code Generation SOP for ISO compliant code
- Generate the Design proposal, Interface specifications, Error handling strategy, and testing plans
- Incremental code generation
- Develop Validation and verification protocol

Iterate as necessary

2. DIGITAL OUTPUTS

2.1 Indicator Outputs (Optocoupler Source)

2.1.1 Ready Light (OUT_READY)

REQ-010 [ASIL-B]

- State HIGH: System in READY state, drive system operational
- State LOW: System not ready (STARTUP, FAULT, EMERGENCY_STOP)

2.1.2 Malfunction Indicator Lamp - MIL (OUT_MIL)

REQ-011 [ASIL-B]

- State HIGH when:
- Fault reported over CAN (motor controller, BMS)
- Internal VCU fault detected
- Limp mode active
- State LOW: No faults present

2.1.3 Brake Applied (OUT_BRAKE_ANY)

REQ-012 [ASIL-C]

- State HIGH: Any brake input active (foot, parking, auxiliary)
- State LOW: No brakes applied

2.1.4 Foot Brake (OUT_BRAKE_FOOT)

REQ-013 [ASIL-C]

- State HIGH: Brake pedal pressed (IN_BRAKE_PEDAL active)
- State LOW: Brake pedal not pressed

2.1.5 Drive Mode - Forward (OUT_GEAR_FWD)

REQ-014 [ASIL-B]

- State HIGH: Drive mode is FORWARD
- State LOW: Drive mode is not forward

2.1.6 Drive Mode - Neutral (OUT_GEAR_NEUTRAL)

REQ-015 [ASIL-B]

- State HIGH: Drive mode is NEUTRAL
- State LOW: Drive mode is not neutral

2.1.7 Drive Mode - Reverse (OUT_GEAR_REV)

REQ-016 [ASIL-B]

- State HIGH: Drive mode is REVERSE
- State LOW: Drive mode is not reverse

2.1.8 Turtle Mode Active (OUT_TURTLE_MODE)

REQ-017 [ASIL-A]

- State HIGH: Reduced performance mode active
- State LOW: Normal performance mode

2.1.9 Reduced Braking Performance Indicator

REQ-018 [ASIL-C]

- State HIGH: Regenerative braking not available
- State LOW: Regenerative braking available

2.2 Power Outputs (MOSFET Sink)

2.2.1 Cooling Fan Outputs (OUT_FAN_1, OUT_FAN_2, ...)

REQ-020 [ASIL-A]

- Control Logic: See Section 6.7
- State HIGH: Temperature > setpoint (C1, C2, etc. per Section 9.2.1)
- State LOW: Temperature < (setpoint - 2°C)

2.2.2 Circulation Water Pump (OUT_PUMP)

REQ-021 [ASIL-A]

- State HIGH when:
- Main contactor active (OUT_MAIN = HIGH), OR
- Pump request received via CAN (see CAN Protocol doc)
- State LOW: Neither condition met

2.2.3 Hill Hold (OUT_HILL_HOLD)

REQ-022 [ASIL-B]

- Control Logic: See Section 6.5
- State HIGH: Hill hold active (holding brake pressure)
- State LOW: Hill hold inactive

2.2.4 Precharge (OUT_PRECHARGE)

REQ-023 [ASIL-D]

- Control Logic: See Section 6.8
- State HIGH: Precharge sequence active
- State LOW: Precharge complete or not active

2.2.5 Main Contactor (OUT_MAIN)

REQ-024 [ASIL-D]

- Control Logic: See Section 6.8
- State HIGH: High voltage bus enabled (precharge complete)
- State LOW: High voltage bus disabled

2.2.6 Charging Active (OUT_CHARGING)

REQ-025 [ASIL-B]

- State HIGH: Vehicle in charging mode (see CAN Protocol doc)
- State LOW: Not charging

2.2.7 Accessory Power (OUT_ACCESSORY)

REQ-026 [ASIL-A]

- State HIGH: High voltage bus enabled (precharge complete) OR Tow mode active (see Section 6.4)
- State LOW: High voltage bus disabled

2.2.8 Audible Alarm (OUT_BUZZER)

REQ-027 [ASIL-B]

- State HIGH: Request for audible alarm
- State LOW: No request for alarm

2.3 Regulated 5V Outputs

2.3.1 Hardwire Throttle Enable

REQ-028 [ASIL-D]

- Dual channel: 2 outputs, one for each sensor
- State HIGH: Complete (closed) circuit to throttle pedal power 5V
- State LOW: Open circuit to throttle pedal power 5V

2.3.2 Sensor Power

REQ-029 [ASIL-C]

- State HIGH: Complete (closed) circuit to sensor power 5V
- State LOW: Open circuit to sensor power 5V

2.3.3 Sensor ground for throttle

- State LOW: always grounded, but monitored for faults

3. DIGITAL INPUTS

All inputs from optocouplers, default state LOW unless specified. Active = HIGH, Inactive = LOW.

3.1 Control Inputs

3.1.1 Run Mode (IN_RUN)

REQ-030 [ASIL-D]

- HIGH: Drive mode requested (Master ON)
- LOW: Master OFF

3.1.2 Brake Pedal Applied (IN_BRAKE_PEDAL)

REQ-031 [ASIL-D]

- HIGH: Brake pedal pressed (affirmative input)
- LOW: Brake pedal not pressed

3.1.3 Brake Pedal Released (IN_BRAKE_RELEASED)

REQ-032 [ASIL-C]

- HIGH: Brake pedal at top of stroke (negative input)
- LOW: Brake pedal not at rest position

3.1.4 Parking Brake Applied (IN_PARKING_BRAKE)

REQ-033 [ASIL-C]

- HIGH: Parking brake engaged
- LOW: Parking brake released

3.1.5 Auxiliary Brake Applied (IN_AUX_BRAKE)

REQ-034 [ASIL-C]

- HIGH: Auxiliary brake system engaged
- LOW: Auxiliary brake not engaged

3.1.6 Turtle Mode Toggle (IN_TURTLE_TOGGLE)

REQ-035 [ASIL-A]

- Type: Momentary button
- Action: Each press toggles turtle mode ON/OFF
- Debounce: 50ms

3.1.7 Override Mode (IN_OVERRIDE)

REQ-036 [ASIL-B]

- HIGH: Allow drive system operation despite most faults (see Section 6.9)
- LOW: Normal fault response

3.1.8 Disable Drive (IN_DISABLE_DRIVE)

REQ-037 [ASIL-D]

- HIGH: Driving prohibited (force torque = 0)
- LOW: Driving permitted

3.1.9 ABS Active (IN_ABS_ACTIVE)

REQ-038 [ASIL-D]

- HIGH: ABS system requests zero wheel torque
- LOW: ABS not active

3.1.10 Tow Mode (IN_TOW_MODE)

REQ-039 [ASIL-A]

- HIGH: Tow mode requested (see Section 6.4)
- LOW: Normal mode

3.2 Transmission Shift Inputs (Momentary)

3.2.1 Forward Request (IN_SHIFT_FWD)

REQ-040 [ASIL-C]

- Type: Momentary button
- Action: Request FORWARD gear mode
- Debounce: 50ms

3.2.2 Neutral Request (IN_SHIFT_NEUTRAL)

REQ-041 [ASIL-C]

- Type: Momentary button
- Action: Request NEUTRAL gear mode
- Debounce: 50ms

3.2.3 Reverse Request (IN_SHIFT_REV)

REQ-042 [ASIL-C]

- Type: Momentary button
- Action: Request REVERSE gear mode
- Debounce: 50ms

3.3 Analog Inputs

3.3.1 Throttle Position Sensor 1 (IN_THROTTLE_1)

REQ-043 [ASIL-D]

- Range: 0.5V to 4.5V (10% margin from 0-5V rails)
- Resolution: 10-bit ADC minimum (12-bit preferred)
- Sample Rate: 500 Hz (2ms interval)

3.3.2 Throttle Position Sensor 2 (IN_THROTTLE_2)

REQ-044 [ASIL-D]

- Range: 0.5V to 4.5V (10% margin from 0-5V rails)
- Resolution: 10-bit ADC minimum (12-bit preferred)
- Sample Rate: 500 Hz (2ms interval)

3.3.3 Aux Temperature Input (x2)

REQ-045 [ASIL-A]

• Range: 0.5V to 4.5V (10% margin from 0-5V rails)

• Resolution: 10-bit ADC minimum

---

4. SYSTEM STATE MACHINE

4.1 State Definitions

4.1.1 OFF

REQ-050 [ASIL-D]

- Description: VCU powered down
- Outputs: All outputs LOW
- Entry: Power removed

4.1.2 POST (Power On System Test)

REQ-051 [ASIL-D]

- Description: System initialization and self-test
- Duration: 2-5 seconds
- Outputs: All outputs disabled
- Activities: Execute tests per Appendix 1
- Safe State Alignment: Fault level or STANDBY

4.1.3 STANDBY

REQ-052 [ASIL-C]

- Description: Parked, master switch OFF, or tow mode active
- Outputs: All outputs disabled except when tow mode active (see Section 6.4)
- Activities: Monitor inputs, faults, CAN communication
- Special Mode: Tow mode (REQ-105-106): (Option)
  - OUT_ACCESSORY = HIGH
  - OUT_MAIN = LOW
  - OUT_READY flashing 2Hz
  - Bypasses BMS fault checks
- Safe State Alignment: Non-operational state

4.1.4 READY

REQ-053 [ASIL-D]

- Description: Normal operation, drive system functional
- Outputs: OUT_READY = HIGH, others as required by process
- Activities:
  - Throttle input processing
  - Torque command generation
  - All safety checks active
  - Auxiliary systems operational

- Safe State Alignment:
  - Default mode = Safe State 1 (full propulsion, no faults)
  - If Alarm Level 1 active = Safe State 1 with MIL (warning only)
  - If Alarm Level 2 active = Safe State 2 (turtle mode forced, OUT_TURTLE_MODE = HIGH, OUT_MIL = HIGH)
  - If Alarm Level 3 active = Safe State 3 (timer active per REQ-149, OUT_BUZZER = HIGH, OUT_MIL = HIGH)

4.1.5 TRIPPED

REQ-054 [ASIL-D]

- Description: Recoverable fault detected, attempting automatic recovery
- Outputs: OUT_MIL = HIGH
- Torque: Forced to 0%
- Activities:
  - Attempting automatic recovery
  - Logging fault events
  - Monitoring for valid sensor data
- Fault Types:
  - Single sensor faults (one sensor out of range while other valid on throttle)
  - Throttle plausibility violations (correlation, gradient, stuck detection)
  - Recoverable CAN message validation errors
- Safe State Alignment: Degraded mode with automatic recovery to Safe State 1
- Recovery: Requires continuous valid operation per REQ-064

4.1.6 FAULT

REQ-055 [ASIL-D]

- Description: Alarm level > 0
- Outputs: depend on level OUT_MIL = HIGH
- Torque: If Alarm level >1 All drive functions disabled
- Activities:
  - Logging fault
  - Monitoring battery current for decay (REQ-152)
  - OUT_MAIN opens per REQ-152-153 after current <20A or timeout if disconnecting
  - Waiting for manual reset (key cycle or power cycle per fault severity)
- Safe State Alignment: depends on alarm level
- Reset Requirements: Per REQ-154-155 and REQ-066

4.2 State Transition Conditions

4.2.1 OFF → STANDBY

REQ-060 [ASIL-D]

- Trigger: Power applied
- Requirements:

  - Power-On System Test pass (Appendix 1)
  - Power supply stable
  - CAN responding

4.2.2 STANDBY → READY (modified)

REQ-061 [ASIL-D]

- Trigger: IN_RUN goes HIGH (key ON) AND IN_TOW_MODE = LOW
- Requirements: Power supply stable
- Activities: Precharge process (Section 6.8)
- Note: If IN_TOW_MODE = HIGH when IN_RUN = HIGH, remain in STANDBY with tow mode active per REQ-105-106 (option)
- Continuous checks
  - Both throttle sensors reading correct voltage
  - Sensors agree within configured tolerance (REQ-151)
  - Motor controller CAN responding
  - BMS CAN responding
  - Fault detection
- Transition: Enter READY state in Safe State 1 configuration

4.2.4 READY → TRIPPED

REQ-063 [ASIL-D]

- Trigger (any recoverable fault):
  - Throttle sensors disagree > configured tolerance (default 10%, REQ-151)
  - Single sensor voltage <0.5V or >4.5V (other sensor remains valid)
  - Sensor gradient exceeds configured limit (default 1.33% per 2ms, REQ-151)
  - Sensor stuck: variance < configured minimum when throttle > (configured deadband + 3%) (default 0.2% variance over 100ms, REQ-151)
  - Single CAN message validation failure (CRC or counter error)
  - Error state reported on CAN.
- Transition: Immediate (no delay), torque = 0%

4.2.5 TRIPPED → READY

REQ-064 [ASIL-D]

- Requirements (all must be true):
  - Configured validation period of continuous valid sensor readings (REQ-152)
  - Sensors agree within configured tolerance (default 10%, REQ-151)
  - Throttle position < configured deadband (default 2%, REQ-151)
  - No other faults active
  - Error state on CAN for less than 3 consecutive messages
- Transition: Return to READY state, Safe State 1 configuration

4.2.6 Any State → FAULT

REQ-065 [ASIL-D]

- Trigger (any critical non-recoverable fault):

  - Both throttle sensors out of range simultaneously
  - Motor controller CAN timeout (REQ-154)
  - BMS CAN timeout (REQ-154)
  - System voltage below minimum threshold
  - Watchdog timeout > configured duration (default 100ms, REQ-157)
  - Precharge failure conditions (REQ-113):
    - Voltage mismatch after timeout (REQ-156)
    - Motor controller no response after precharge complete
    - Transition testing process failure
  - Operational self-test failure (REQ-165)
  - Torque tracking error: |commanded - actual| >25% for >100ms
  - BMS Alarm Level 4 received (REQ-151)
- Immediate Actions:
  - Torque reduced (level dependent)
  - OUT_MIL = HIGH
  - OUT_BUZZER = HIGH if alarm level >2
  - Monitor current for decay per REQ-152-153
  - Open OUT_MAIN when current < configured threshold (REQ-155) or timeout (REQ-153) if alarm level >3
- Exception: If in STANDBY with tow mode active, tow mode behavior takes precedence

4.2.7 FAULT → READY

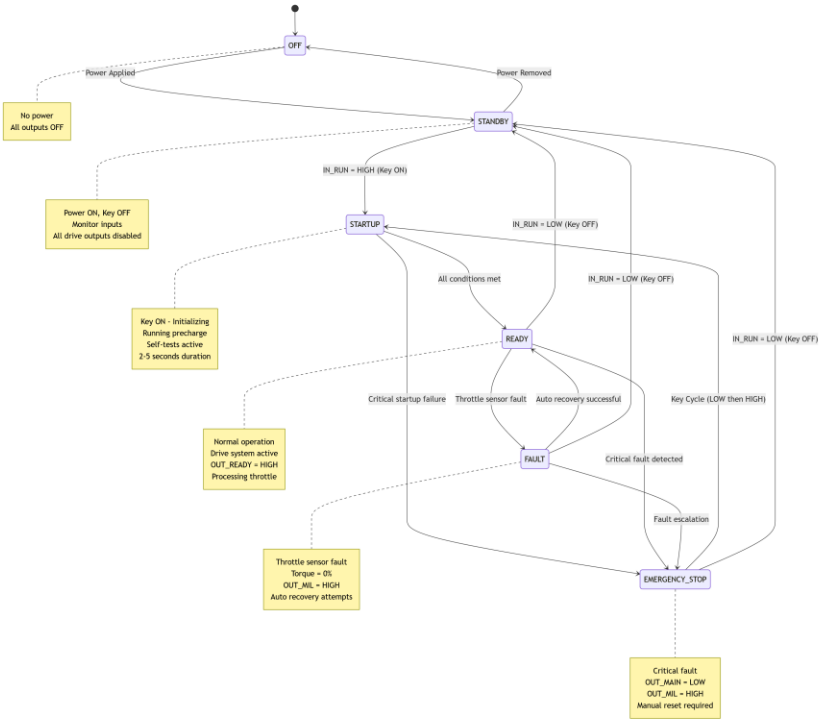
REQ-066 [ASIL-D]

- Power cycle for Alarm Level 4 faults
- Key cycle for Alarm Level 3 faults or other critical faults
- Must pass POST (REQ-062) before transitioning to READY
- IN_TOW_MODE must be LOW

4.3 Additional State Transitions

REQ-067 [ASIL-C] Any READY/FAULT → STANDBY

- Trigger: IN_RUN = LOW (master switch OFF)
- Exception: EMERGENCY_STOP state requires power reset per REQ-066
- Transition: Immediate, all outputs disabled



5. THROTTLE INPUT PROCESSING

5.1 Hardware Configuration

5.1.1 Dual Sensor Architecture

REQ-070 [ASIL-D]

- Two independent analog throttle position sensors (TPS1, TPS2)
- Asymmetric capable inputs (half level)
- Voltage range: 0.5V to 4.5V operating (10% margin from rails)
- ADC resolution: Minimum 12-bit
- Sample rate: 500 Hz (2ms loop time)
- Electrical isolation: RC filters on each input (100Ω + 100nF minimum)

5.1.2 Processing Priority

REQ-071 [ASIL-D]

- Throttle signal processing runs as highest priority task
- Independent from other controller functions
- Maximum latency from sensor read to CAN transmission: 2ms
- Not interrupted by non-critical tasks

5.2 Sensor Validation

Execute these checks every loop iteration (2ms):

5.2.1 Cross-Channel Agreement Check

REQ-072 [ASIL-D]

- Maximum deviation: 10% of normalized full scale (Section 9.6.1)
- Action if violated: Transition to TRIPPED state immediately
- Purpose: Detect wiring fault, sensor failure, or electrical interference

5.2.2 Voltage Range Check

REQ-073 [ASIL-D]

- Valid range: 0.5V to 4.5V
- Rail voltage detection: Reading < 0.5V or > 4.5V indicates:

o Wire break (open circuit)
o Short circuit to ground or Vcc
o Sensor power supply failure

- Action if violated: Transition to TRIPPED state immediately

5.2.3 Gradient Plausibility Check (Physical Limit)

REQ-074 [ASIL-D]

- Physical constraint: Human foot cannot move throttle faster than 100% in 150ms (Under most conditions)
- Per-loop limit: 1.33% per 2ms (100%/150ms × 2ms) adjustable with CAN message to register (per Section 9.6.1)
- Action if violated: Reject new reading, hold previous valid value, log event
- Purpose: Catch electrical spikes or sensor glitches

5.2.4 Sensor Stuck Detection

REQ-075 [ASIL-D]

- Requires high resolution ADC
- Trigger condition: When sensor variance is < 5% (value "freezes")
- Requirement: Sensor value must vary by at least 0.2% over 100ms (per Section 9.6.1)
- Action if violated: Transition to TRIPPED state
- Purpose: Detect frozen sensor or broken signal path

5.3 Signal Processing

5.3.1 Noise Filtering

REQ-076 [ASIL-D]

- Method: Median filter on last 3 samples per sensor
- Purpose: Eliminate single-point electrical noise spikes
- Latency: 6ms (3 samples × 2ms)

5.3.2 Sensor Fusion

REQ-077 [ASIL-D]

- Asymmetric sensors: throttlePosition = (TPS1_normalized + TPS2_normalized) / 2
- Output range: 0% to 100%

5.3.3 Deadband Application

REQ-078 [ASIL-C]

- Threshold: default 2% of full scale (per Section 9.6.1)
- Logic: If throttlePosition < 2%, set to 0%
- Purpose: Eliminate pedal resting position drift

5.4 Fault Recovery

5.4.1 Recovery Requirements

REQ-079 [ASIL-D]

- 500ms of continuous valid sensor readings (per Section 9.6.2)
- Both sensors agree within 10% threshold (per Section 9.6.1)
- Throttle position in deadband (< 2% per Section 9.6.1)
- No other active faults

5.4.2 State Transition

REQ-080 [ASIL-D]

- From TRIPPED → READY
- OUT_MIL clears when fault cleared
- Logging output on CAN

6. TORQUE CONTROL AND SAFETY FUNCTIONS

6.1 Torque Request Generation

6.1.1 Throttle-to-Torque Mapping

REQ-090 [ASIL-C]

Base Calculation:

torqueRequest = throttlePosition ^ responseExponent

Response Modes:

- Normal mode: exponent = 1.0 (linear 1:1 mapping) - configurable per Section 9.1.1
- Turtle mode: exponent = value between 0 and 1 set via CAN - default 0.7 per Section 9.1.1

6.1.2 Torque Rate Limiting

REQ-091 [ASIL-C]

- Ramp-up rate: 200%/second (0→100% in 500ms) - configurable per Section 9.1.2
- Ramp-down rate: 400%/second (100%→0% in 250ms) - configurable per Section 9.1.2
- Purpose: Smooth torque transitions, prevent jerk

6.2 Battery Current Limiting (DCL/CCL)

6.2.1 BMS CAN Interface

REQ-092 [ASIL-D]

Receive from BMS (see CAN Protocol doc for message format):

- DCL: Discharge Current Limit [Amps]
- CCL: Charge Current Limit [Amps]

BMS Timeout Handling:

6.2.2 DCL Limiting

REQ-093 [ASIL-D]

- If IN_OVERRIDE = HIGH: allow limited operation in turtle mode (ref 6.9.1)

Display Warning: If performance from DCL is reduced, turn on Turtle Mode output (OUT_TURTLE_MODE per Section 2.1.8).

- Send CAN message for reduced performance to HMI

6.2.3 Motor Controller Feedback

REQ-094 [ASIL-D]

Receive from Motor Controller (see CAN Protocol doc):

- Actual motor current [Amps]
- Actual torque output [%]
- Update rate: 100 Hz (10ms)

6.2.4 Regenerative Braking

REQ-095 [ASIL-C]

```
Algorithm:
if (footbrake confirmed AND CCL above limit AND RPM > 500):
    baseRegen% = regenStrength // configurable parameter (default 30% per Section 9.1.2)
    Scale regen with RPM
    rpmScale = 1.0

    regenRequest% = baseRegen% × rpmScale
else:
    regenRequest% = 0%
```

6.2.5 CCL Reduction Handling

REQ-096 [ASIL-C]

If CCL is below setpoint (default = 250A per Section 9.1.2)

- Disable all regenerative braking
- Route brake pedal to friction brakes only
- Send message on CAN for reduced brake performance.

- T Turn on BRAKE PERFORMANCE REDUCED output (OUT per Section 2.1.9)

6.2.6 Temperature-Based Derating

REQ-097 [ASIL-B]

The BMS is responsible for the calculation of CCL and DCL. Any temperature compensation necessary will be processed by the BMS.

6.3 Safety Interlocks

6.3.1 Unintended Acceleration Prevention

REQ-100 [ASIL-D]
Execute every loop iteration (2ms):

```
Unintended Motion Detection:
IF all conditions true:
1. Vehicle moving: abs(motorRPM) > 100 RPM (per Section 9.6.3)
2. Significant torque: abs(actualTorque) > 10% (per Section 9.6.3)
3. Torque direction matches RPM direction (driving, not braking)
4. Throttle NOT pressed: in “deadband” and gear NOT in neutral.
THEN:
- Set flag: unintended torque Detected = TRUE (see CAN protocol)
- Force torqueRequest = 0%
- Log safety event
```

Clear Condition:

- Brake applied AND vehicle stopped (RPM near zero)
- Gear in neutral

6.3.2 Brake Pedal Override (Highest Priority)

REQ-101 [ASIL-D]
IF (IN_BRAKE_PEDAL = HIGH):
- Override all throttle input
- No exceptions or delays
- Note: if brake sensor fails, the vehicle will not shift into gear.

6.3.3 Drive Disable Interlock

REQ-102 [ASIL-D]
IF (IN_DISABLE_DRIVE = HIGH):
- Force torqueRequest = 0%
- Ignore throttle input
- Log disable event through CAN

6.3.4 ABS Interlock

REQ-103 [ASIL-D]
IF (IN_ABS_ACTIVE = HIGH):
- Force torqueRequest = 0%
- Allow ABS system to control wheel speed

6.3.5 Gear Mode Interlocks

REQ-104 [ASIL-D]
Park/Neutral:
IF (Park brake ON): or (Foot brake off)
- Ignore drive and reverse buttons
- Ignore throttle input

IF (gearMode = NEUTRAL):
- Force torqueRequest = 0%
- Ignore throttle input

Reverse Direction Conflict:
IF (gearMode = REVERSE) AND (motorRPM > 200):
- Force torqueRequest = 0%
- Log CAN message flag for directional fault.

6.4 Tow Mode (optional)

6.4.1 Activation

REQ-105 [ASIL-A]
IF (IN_TOW_MODE = HIGH) AND (IN_RUN = HIGH): only from STANDBY MODE
Tow mode is intended to be key lockable and accessible only for service personnel.
If TowMode input goes high in any other mode, it will be ignored until the key is cycled.
- Transition to TOW_MODE state
- OUT_MAIN = LOW (disable high voltage)
- OUT_ACCESSORY = HIGH

Monitor battery current keeps under set value.

6.4.2 Behavior

REQ-106 [ASIL-A]
- Ignores all fault conditions
- Motor controller disabled
- Allows vehicle to be pushed with power steering and air

6.5 Hill Hold

6.5.1 Activation Conditions (all must be true)

REQ-107 [ASIL-B]
IF:
- motorRPM < 2 RPM (vehicle nearly stopped - per Section 9.4.2)

AND
- IN_BRAKE_PEDAL = HIGH

AND

- throttlePosition is in deadband
THEN:
- OUT_HILL_HOLD = HIGH

6.5.2 Deactivation Conditions (either)

REQ-108 [ASIL-B]
IF:
(gearMode = FORWARD OR gearMode = REVERSE) AND
(throttlePosition > 10% OR abs(actualTorque) > Qx)
THEN:
- OUT_HILL_HOLD = LOW
With configurable torque threshold Qx = 15% default (see Section 9.4.1)

6.6 Rollaway Alarm

6.6.1 Activation

REQ-109 [ASIL-B]
IF (gearMode = NEUTRAL) AND (ALL brake signals LOW):
- OUT_BUZZER = HIGH
ELSE:
- OUT_BUZZER = LOW

6.7 Cooling Fan Control

6.7.1 Algorithm (per fan output)

REQ-110 [ASIL-A]
IF (assignedTemperature > Cx):
- OUT_FAN_x = HIGH

IF (assignedTemperature < Cx - 2°C):
- OUT_FAN_x = LOW
Where:
• assignedTemperature = motor temp, inverter temp, or other monitored temperature
• Cx = configurable setpoint per fan:
o C1 = 70°C default for motor winding (Section 9.2.1)
o C2 = 65°C default for inverter (Section 9.2.1)
• 2°C hysteresis prevents rapid cycling

6.7.2 Temperature Sources

REQ-111 [ASIL-A]
• Motor winding temperature (from motor controller CAN)
• Inverter temperature (from motor controller CAN)
• Additional sensors as configured (see CAN Protocol doc)
• Auxiliary analog temperature sensor inputs (Section 3.3.3)

6.8 Precharge

6.8.1 Sequence

REQ-112 [ASIL-D]

System tests in the sequence from standby to startup run continuously. If at any time a test fails, state moves to Fault mode, the precharge process is ended.

Step 1: Power-On

- IN_RUN = HIGH
- Start testing sequence
- Check all contactors open

Step 2: Initiate Precharge

- Start watching voltages from Voltage transducer (see CAN Protocol doc) and BMS pack voltage
- OUT_PRECHARGE = HIGH (close the precharge contactor)

Step 3: Monitor Voltage Rise and System Tests

- Wait for: transducerVoltage ≈ bmsVoltage within 5% (per Section 9.8.1)
- Timeout: 10 seconds (per Section 9.8.1)
  (if not matched by timeout, transition to EMERGENCY_STOP)

Step 4: Close Main Contactor

- Voltages matched
- OUT_MAIN = HIGH

Step 5: Complete Precharge

- Wait 200ms (contactor settling time)
- OUT_PRECHARGE = LOW

Step 6: Wait for Drive Systems

- Wait for motor controller READY status (see CAN Protocol doc)
- End startup testing, transition to regular monitoring

Step 7: System Ready

- Transition to READY state
- OUT_READY = HIGH

6.8.2 Fault Conditions

REQ-113 [ASIL-D]

• If precharge voltage does not match within 10 seconds (per Section 9.8.1) → EMERGENCY_STOP
• If motor controller does not respond → EMERGENCY_STOP
• If transition testing process finds a failure → EMERGENCY_STOP
• Set fault code, Log data and results to CAN

6.9 Override Mode

- **6.9.1 Function**
  REQ-114 [ASIL-B]
  IF (IN_OVERRIDE = HIGH):

Allow drive system operation at reduced performance for limited time despite:

- MIL request from CAN message
- BMS fault reported
- BMS CAN timeout

Does NOT override:

- Throttle sensor faults
- Motor controller CAN timeout
- Critical safety interlocks (brake override, unintended motion)

6.9.2 Purpose

REQ-115 [ASIL-B]

- Emergency "limp" capability
- Allow vehicle operation with degraded battery management
- Operator assumes responsibility for safe operation
- Uses a timer. Momentary on allows 15 seconds of HV connection (per Section 9.10.1)

6.10 Traction Control

6.10.1 Slip Detection

REQ-116 [ASIL-B]

Detect wheel slip when:

RPM changes more than a set value over a set time period
Values calibrated in section 9.3

6.10.2 Slip Response

REQ-117 [ASIL-B]

IF slip detected on motor:

- Reduce torque to slipping motor by 20% (per Section 9.3.3)
- Hold reduced torque for 500ms (per Section 9.3.3)
- Gradually restore torque over 1 second (per Section 9.3.3)
- Log traction control event to CAN

---

7. CAN BUS COMMUNICATION

7.1 CAN Bus Architecture

7.1.1 Vehicle CAN (CAN1)

REQ-120 [ASIL-C]

- Connected Devices: VCU, BMS, brake controller, displays, other vehicle systems

- Baud Rate: 250 kbps (see CAN Protocol doc for confirmation)
- Purpose: Vehicle-wide data sharing

7.1.2 Motor Controller CAN (CAN2)

REQ-121 [ASIL-D]

- Connected Devices: VCU, motor controller(s) ONLY
- Baud Rate: TBD (see CAN Protocol doc)
- Purpose: High-priority drive commands, isolated from vehicle bus

7.2 Transmitted Messages (from VCU)

REQ-122 [ASIL-D]

All message IDs, formats, and update rates are defined in the VCU CAN Protocol Specification (Spreadsheet).

---

8. DIAGNOSTIC AND FAULT MANAGEMENT

8.1 Document Control

8.1.1 Document ID

REQ-811 [ASIL D]

- CANbus protocol
- Fault code table

  Document versions are on the revisions page of this document.

8.1.2 Related Safety Goals

REQ-812 [ASIL D]

- HARA document

8.1.3 Assumption of Use

REQ-813 [ASIL D]

- Passenger conveyance in a closed park environment with a maximum speed of 25MPH, operated by a trained driver. NO highway use. (speed set in section 9.1.1)

8.2 Safe State Definitions

8.2.1 Safe State Definitions

REQ-821 [ASIL D]

The VCU shall support the following safe states:

- Safe State 1 - Warning Active: Full propulsion available with driver notification
- Safe State 2 - Power Limited: Reduced propulsion power (turtle mode), vehicle can continue driving to safe location
- Safe State 3 - Controlled Stop: Propulsion available for 30 seconds to allow driver to move to safe location, then disabled. HV remains on for steering/braking
- Safe State 4 - Immediate Disable: Propulsion disabled immediately, HV contactors opened after current decay, vehicle coasts to stop

8.2.2 Transition Requirement

REQ-822 [ASIL D]

The VCU shall transition to the appropriate safe state based on the alarm level received from the BMS or detected internal VCU fault.

8.3 Fault Tolerant Time Interval (FTTI)

8.3.1 FTTI Values

REQ-831 [ASIL D]

The VCU shall achieve the following maximum FTTI for each hazardous event:

- Hazardous Event: Unintended Acceleration
  - VCU FTTI: 100ms
  - Rationale: H-01 (ASIL C) / SG-01 (VCU detects fault & commands zero torque)
- Hazardous Event: VCU Response to Alarm level 4
  - VCU FTTI: 100ms
  - Rationale: H-05 (ASIL D) / SG-03 (VCU must command Safe State 4 immediately upon receiving Level 4 alarm from BMS)
- Hazardous Event: VCU Internal Processor Failure
  - VCU FTTI: 50ms
  - Rationale: H-10 (ASIL D) / SG-07 (VCU self-diagnostics/external watchdog must initiate safe state)

8.3.2 Timing Consistency

REQ-832 [ASIL D]

All timing requirements in this document shall be derived from and consistent with the FTTI values defined above.

8.4 BMS Alarm Level Interface

8.4.1 CAN Message Reception

REQ-841 [ASIL C]

The VCU shall receive BMS alarm level via CAN message (Alarm Level: 0=None, 1=Warning1, 2=Warning2, 3=Stop, 4=Disable)

8.4.2 BMS CAN Message Period

REQ-842 [ASIL C]

The VCU shall expect BMS alarm level message at 10ms

8.4.3 CAN Message Content

REQ-843 [ASIL C]

The BMS alarm level message shall include:

- Rolling counter (4-bit, incrementing 0-15)
- CRC-8 checksum per SAE J1850

8.4.4 Message Validation

REQ-844 [ASIL C]

The VCU shall validate each received BMS alarm level message for:

- Sequence counter correctness (no skipped messages, no repeated messages)
- CRC/checksum correctness
- Alarm level value within valid range (0-4)
- Message received within expected cycle time

8.4.5 Validation Failure Response

REQ-845 [ASIL C]

If message validation fails, the VCU shall maintain previous valid alarm level and increment fault counter

- After 5 consecutive validation failures, the VCU shall escalate to Alarm Level 2
- The fault counter does not zero on reception of a valid message, but decrements by 1 until it reaches zero

8.4.6 Communication Timeout Detection

REQ-846 [ASIL C]

If no valid BMS alarm level message is received within 500ms, the VCU shall detect a communication timeout fault.

8.4.7 BMS Communication Timeout Response

REQ-847 [ASIL C]

Upon BMS communication timeout:

- The VCU shall Trigger Warning Level 1 within 100ms
- If timeout persists for 3 seconds, escalate to Stop Level (Warning Level 3)

8.5 VCU Response to Alarm Levels

8.5.1 Alarm Level 1 Response

REQ-851 [ASIL B]

When BMS alarm level = 1, the VCU shall transition to Safe State 1 and:

- Turn on MIL output within 100ms
- Output CAN message that indicates warning level to HMI

8.5.2 Alarm Level 1 Propulsion

REQ-852 [ASIL B]

The VCU shall NOT restrict propulsion in Alarm Level 1.

8.5.3 Alarm Level 2 Response

REQ-853 [ASIL C]

When BMS alarm level = 2, the VCU shall transition to Safe State 2 and:

- Turn on MIL output within 200ms
- Output CAN message that indicates warning level to HMI
- VCU will change to limited performance within 500ms

8.5.4 Alarm Level 2 Propulsion

REQ-854 [ASIL C]

The VCU shall allow propulsion with limited performance in Alarm Level 2.

8.5.5 Alarm Level 3 (Stop) Response

REQ-855 [ASIL D]

When BMS alarm level = 3, the VCU shall transition to Safe State 3 and:

- Output CAN message that indicates stop level to HMI
- Turn on MIL within 100ms
- Turn on audible alarm output within 100ms

8.5.6 Alarm Level 3 Drive Disable

REQ-856 [ASIL D]

After delay from Alarm Level 3 activation, the VCU shall command motor controller to disable drive (zero torque, no regeneration).

- Delay default: 15 seconds (adjustable in calibration variables) *need ref!*

8.5.7 Alarm Level 3 HV Contactor State

REQ-857 [ASIL D]

The VCU shall maintain HV contactors closed during Alarm Level 3 to preserve normal operation of all other components.

8.5.8 Alarm Level 4 (Disable) Response

REQ-858 [ASIL D]

When BMS alarm level = 4, the VCU shall transition to Safe State 4 and:

- Command motor controller to disable immediately (zero torque, no regeneration) within 100ms
- Output CAN message that indicates stop level to HMI
- Turn on audible alarm output within 100ms

8.5.9 Alarm Level 4 Current Monitoring

REQ-859 [ASIL D]

After drive disable command, the VCU shall monitor battery pack current for 10 seconds

8.5.10 Alarm Level 4 Contactor Opening

REQ-8510 [ASIL D]

The VCU shall command HV contactors to open when EITHER condition is met:

- Battery pack current < 20A for 500ms continuous
- Elapsed time since Alarm Level 4 activation = 10 seconds
- Reference 9.7.1

8.5.11 Alarm Level 4 Contactor Re-closure Prevention

REQ-8511 [ASIL D]

Once HV contactors are opened due to Alarm Level 4, the VCU shall prevent contactor re-closure until ALL of the following are met:

- Full power cycle
- POST pass successfully

8.5.12 Alarm Level De-escalation

REQ-8512 [ASIL D]

De-escalation from Alarm Level 4 (Disable) shall require full reset and shall not occur automatically.

8.6 Special Hazard Cases

8.6.1 High Voltage Isolation Fault Detection

REQ-861 [ASIL D]

The VCU shall receive BMS alarm level 4 in the event of an isolation fault.

8.6.2 High Voltage Isolation Fault Response

REQ-862 [ASIL D]

Upon detection of HV isolation fault (alarm level 4) the VCU shall immediately transition to Safe State 4

8.6.3 Fire Detection Response

REQ-863 [ASIL D]

Upon detection of a thermal event (alarm level 4) the VCU shall immediately transition to Safe State 4

8.7 Timing Requirements

8.7.1 Execution Frequency

REQ-871 [ASIL D]

The VCU safety monitoring and response functions shall execute at minimum frequency 10Hz (100ms cycle).

8.7.2 Response Time

REQ-872 [ASIL D]

Time from BMS alarm level message reception to VCU safety response action initiation shall not exceed 100ms.

8.7.3 FTTI Consistency

REQ-873 [ASIL D]

These timing requirements shall be consistent with FTTI values specified in 8.3.1

8.8 Diagnostic Coverage

8.8.1 Coverage Metrics

REQ-881 [ASIL D]

The VCU safety mechanisms shall achieve minimum diagnostic coverage per ASIL requirements:

- Single Point Fault Metric (SPFM): >90% for ASIL C or >99% for ASIL D
- Latent Fault Metric (LFM): >60% for ASIL C or >90% for ASIL D

8.8.2 Safety Mechanisms

REQ-882 [ASIL D]

The VCU shall implement the following safety mechanisms to achieve required diagnostic coverage:

- Program flow monitoring (watchdog)
- RAM test (March algorithm)
- Contactor feedback verification
- CAN message validation (sequence counter, CRC)
- Plausibility checks on sensor inputs

8.8.3 Self-Test Requirements

REQ-883 [ASIL D]

The VCU shall perform self-test of safety-critical monitoring paths at:

- Power-up (before enabling HV contactors)
- Every 10 seconds during operation for latent fault detection

8.8.4 Self-Test Fault Response

REQ-884 [ASIL D]

If self-test detects a fault in safety mechanisms, the VCU shall prevent HV contactor closure (if at power-up) or transition to Safe State 4 (if during operation).

8.9 Freedom From Interference (FFI)

8.9.1 Software Partitioning

REQ-891 [ASIL D]

The VCU software architecture shall implement partitioning between ASIL-rated safety functions and QM (Quality Management) non-safety functions per ISO 26262-6 Table 1.

8.9.2 Memory Protection Unit

REQ-892 [ASIL D]

Memory partitioning shall be implemented using the processor's MPU (Memory Protection Unit).

8.9.3 Protected Memory Regions

REQ-893 [ASIL D]

The following memory regions shall be protected from non-safety function access (separate core):

- Safety-critical variables (alarm level, timing counters)
- Safety function code sections
- Interrupt vectors for safety-critical interrupts
- Motor controller communication buffers

8.9.4 Priority Scheduling

REQ-894 [ASIL D]

Safety-critical functions shall have guaranteed execution time via priority scheduling.

8.9.5 Execution Timing Monitoring

REQ-895 [ASIL D]

The VCU shall monitor execution timing and detect if safety functions miss their execution deadline by more than 10%. Detection shall trigger immediate processor reset and safe state transition.

8.9.6 Inter-Partition Communication

REQ-896 [ASIL D]

Communication between safety and non-safety software elements shall use message passing with data validation.

8.9.7 CAN Message Priority

REQ-897 [ASIL C]

Safety-critical CAN messages shall be transmitted with priority over non-safety messages using CAN message ID priority assignment.

8.10 External Monitoring

8.10.1 External Safety Element

REQ-8101 [ASIL D]

The VCU shall be monitored by external safety element (one of the following):

- External watchdog IC via watchdog trigger
- Secondary monitoring processor via watchdog trigger

8.10.2 Watchdog Signal

REQ-8102 [ASIL D]

The VCU shall provide watchdog/monitoring signal at frequency minimum 1Hz toggling pattern.

8.10.3 Failure Response

REQ-8103 [ASIL D]

If external monitoring detects VCU failure, the external safety element shall disconnect contactors

8.11 Diagnostic Trouble Codes and Event Logging

8.11.1 DTC Generation

REQ-8111 [ASIL D]

The VCU shall generate Diagnostic Trouble Codes (DTCs) per the document "ZCC faults list".

8.11.2 DTC Storage

REQ-8112 [ASIL C]

DTCs shall be stored in non-volatile memory.

8.11.3 Event Data Transmission

REQ-8113 [ASIL C]

The VCU shall transmit safety-relevant event data via CAN message to external logger when any of the following occur:

- Alarm level change (1, 2, 3, or 4)

- communication timeout
- A contactor is closed when it should be open

8.11.4 Event Data Content

REQ-8114 [ASIL C]

Event data transmitted to logger shall include:

- CAN messages that contain fault flags
- Critical battery data
- Critical drive data

8.11.5 Logger Verification

REQ-8115 [ASIL B]

The VCU shall verify external CAN logger is present and receiving messages via periodic heartbeat message from logger.

- The CAN edge transmits a configurable CAN message
- This requirement can be toggled on and off in calibration configuration

8.12 System Architecture Requirements

8.12.1 Control Channels

REQ-8121 [ASIL D]

Each external component shall be commanded by exactly one control source. The following components shall be controlled exclusively by VCU:

- HV contactors (open/close commands)
- Motor controller (torque commands, enable/disable)
- HMI (warning displays, alarms)

8.12.2 BMS Contactor Control Exception

REQ-8122 [ASIL D]

Exception: BMS may open HV contactors independently in emergency conditions. VCU shall detect and respond to BMS-initiated contactor opening within 500ms.

8.12.3 CAN Message ID Assignment

REQ-8123 [ASIL C]

All CAN message IDs shall be uniquely assigned. The same message ID shall not be used for different data content anywhere in the vehicle network. CAN ID assignments are defined in the CAN protocol.

8.12.4 Safety-Critical CAN Message Protection

REQ-8124 [ASIL C]

Safety-critical CAN messages (alarm level, contactor commands, isolation fault) shall use:

- Sequence counter (rolling counter of at least 4-bits)
- CRC checksum of 8-bits
- CRC calculation: Sum of all bits with ID masked with 0xFF

8.13 Verification Requirements

8.13.1 Verification Methods

REQ-8131 [QM]

Each safety requirement in this document shall be verified through combination of:

- Requirements review and inspection
- Failure Mode and Effects Analysis (FMEA)

- Fault Tree Analysis (FTA) for hazardous events
- Hardware-in-Loop (HIL) testing

8.13.2 Timing Verification

REQ-8132 [ASIL D]

Timing requirements (Section 8.7) shall be verified via HIL testing under worst-case load conditions including:

- Maximum CAN bus load

8.13.3 Fault Injection Testing

REQ-8133 [ASIL D]

Fault injection testing shall be performed to verify correct VCU response for:

- All BMS alarm levels (1, 2, 3, 4)
- BMS communication timeout
- BMS message corruption (CRC error, sequence error)
- Motor controller CAN timeout
- Motor controller corruption test

8.13.4 Diagnostic Coverage Verification

REQ-8134 [ASIL D]

Diagnostic coverage (SPFM, LFM) shall be verified through:

- FMEA with diagnostic coverage analysis
- Fault injection testing of safety mechanisms

8.14 Assumptions and Dependencies

8.14.1 Component Assumptions

REQ-8141 [ASIL D]

This VCU safety specification assumes the following system components meet their own safety requirements:

- Component: BMS
  - Assumption: Correctly monitors all cell voltages and temperatures
  - Reference: BMS datasheet
  - Assumption: Transmits accurate alarm level via CAN with <100ms latency
  - Reference: BMS CAN protocol
- Component: Motor Controller
  - Assumption: Responds to disable command within time specified by motor controller
  - Reference: Motor controller spec ID
- Component: HV Contactors
  - Assumption: Open within 50ms of command per contactor datasheet
  - Reference: Contactor spec/datasheet
- Component: CAN Logger
  - Assumption: Logs all CAN messages with <50% capture rate and timestamp accuracy <1ms
  - Reference: Logger spec document ID

8.14.2 Assumption Violation

REQ-8142 [ASIL D]
If any assumption is violated, the VCU safety case shall be re-evaluated per ISO 26262-8 clause 14 (Impact analysis).

9. CONFIGURATION AND CALIBRATION PARAMETERS

9.1 Performance Parameters

9.1.1 Response Curve Exponents

REQ-911 [ASIL-C]

Normal maximum speed adjustment

- Default: 25 mph
- Range: 8 to 80 mph

Normal Mode Exponent:

- Default: 1.0 (linear)
- Range: 0.5 to 2.0
- Units: dimensionless
- Description: Throttle position raised to this power
- <1.0 = gentler initial response
- 1.0 = linear
- 1.0 = aggressive initial response

Curbed Mode Exponent:

- Default: 0.7 (reduced response)
- Range: 0.3 to 1.0
- Units: dimensionless
- Description: Reduces torque response for limited performance mode

9.1.2 Performance Parameters (Non-Safety)

REQ-912 [ASIL-A]

Parameter	Reference	Default	Valid Range	Units
Normal mode response	6.1.1	1.0	0.5 to 2.0	dimensionless
Curb mode response	6.1.1	0.7	0.3 to 1.0	dimensionless
Torque ramp-up rate	6.1.2	200%/s	100 to 400%/s	%/s
Torque ramp-down rate	6.1.2	400%/s	200 to 800%/s	%/s
Regen strength	6.2.4	30%	10 to 50%	% torque
Min CCL setpoint	6.2.5	250	150 to 500	Amps

9.2 Temperature Control Setpoints

9.2.1 Fan Control Setpoints

REQ-921 [ASIL-A]

Fan 1 Setpoint (C1):

- Default: 70°C
- Range: 30°C to 90°C
- Description: Motor winding temperature threshold
- Reference: Section 6.7.1

Fan 2 Setpoint (C2):

- Default: 65°C
- Range: 30°C to 90°C
- Description: Inverter temperature threshold
- Reference: Section 6.7.1
- Hysteresis:
- Fixed: 2°C (fan turns OFF at setpoint - 2°C)
- Reference: Section 6.7.1

9.3 Traction Control Parameters

9.3.1 Slip Detection Threshold (Sx)

REQ-931 [ASIL-B]

Motor RPM Delta:

- Default: 500 RPM
- Range: 100–1000 RPM
- Description: Change in RPM that indicates wheel slip
- Reference: Section 6.10.1

9.3.2 Slip Detection Time Window (Sy)

REQ-932 [ASIL-B]

Time Period:

- Default: 100 ms
- Range: 50–500 ms
- Description: Time window over which RPM delta is measured
- Reference: Section 6.10.1
- Combined Logic:
- If motor RPM increases by >Sx in time <Sy → slip detected

9.3.3 Slip Response Parameters

REQ-933 [ASIL-B]

Torque Reduction percentage

- Default: 20%
- Range: 10–50%
- Description: Amount to reduce torque when slip detected
- Reference: Section 6.10.2

Hold Duration:time

- Default: 500 ms
- Range: 250–2000 ms
- Restore Ramp Rate:
- Default: 1 second
- Range: 0.5–3 seconds

9.4 Hill Hold Parameters

9.4.1 Activation Threshold (Qx)

REQ-941 [ASIL-B]

Torque Threshold percent

- Default: 15%
- Range: 5–30%
- Description: Torque level at which hill hold releases

- Reference: Section 6.5.2

9.4.2 Activation Conditions

REQ-942 [ASIL-B]

RPM Threshold:

- Default: 2 RPM
- Range: 0–10 RPM
- Description: RPM at which hill hold engages.
- Brake Required: IN_BRAKE_PEDAL must be HIGH
- Reference: Section 6.5.1

9.5 Current Limiting Parameters

9.5.1 Current-to-Torque Conversion

REQ-951 [ASIL-D]

Calibration Constant Amps/percent

- Default: 5.5 A per 1% torque
- Range: 3.0–10.0 A/%
- Description: System-specific current draw per torque percent
- Reference: Section 6.2.2

9.5.2 Soft Limiting Thresholds

REQ-952 [ASIL-C]

- Values approaching CCL trigger reduced performance

9.6 Throttle Safety Parameters

9.6.1 Throttle Sensor Validation

REQ-961 [ASIL-D]

Correlation Tolerance:

- Default: 10%
- Range: 5–15%
- Gradient Limit:
- Default: 1.33% per 2ms
- Range: 0.5–3.0% per 2ms

Stuck Detection Variance:

- Default: 0.2% over 100ms
- Range: 0.1–1.0%
- Deadband:
- Default: 2%
- Range: 1–5%

9.6.2 Sensor Fault Recovery Time

REQ-962 [ASIL-D]

Validation Period:

- Default: 500 ms
- Range: 200–2000 ms
- Description: Continuous valid readings required before recovery from FAULT state
- Reference: Section 5.4.1, 4.2.5

9.6.3 Unintended Motion Detection

REQ-963 [ASIL-D]

RPM Threshold:

- Default: 100 RPM
- Range: 50–500 RPM
- Torque Threshold:
- Default: 10%
- Range: 5–20%

9.7 CAN Bus Parameters

9.7.1 Timeout Thresholds

REQ-971 [ASIL-D]

Motor Controller Timeout:

- Default: 100 ms
- Range: 50–5000 ms
- BMS Timeout:
- Default: 100 ms
- Range: 50–5000 ms
- All CAN timeouts: MIL illumination per 8.4.3

9.7.1 Timeout response

REQ-972 [ASIL-C]

Level 3 alarm to drive disable

- Delay default: 15s
- Range: 10–100s

Level 4 alarm to drive timeout:

- Delay default: 15s
- Range: 0–100s

Level 4 alarm to disconnect

- Monitor ESS current; open contactors if below threshold
- Default: 20A
- Range: 1–100A

9.8 Precharge Parameters

9.8.1 Precharge Thresholds

REQ-981 [ASIL-D]

Voltage Matching Tolerance:

- Default: 5%
- Range: 2–10%
- Precharge Timeout:
- Default: 10s
- Range: 5–30s

9.9 Watchdog Parameters

9.9.1 Watchdog Configuration

REQ-991 [ASIL-D]

Timeout Period:

- Default: 100 ms
- Range: 50–500 ms
- Pet Frequency:
- Every control loop (2ms)
- Must be <50% of timeout period

9.10 Override Mode Parameters

9.10.1 Override Timer

REQ-9101 [ASIL-B]

Maximum Override Duration:

- Default: 15s
- Range: 5–60s

9.10.2 Override Performance Limits

REQ-9102 [ASIL-B]

- Torque Limit: Same as curb mode

9.11 Configuration Management

9.11.1 EEPROM Memory Map

REQ-9111 [ASIL-D]

- Safety-relevant memory verified by checksum on startup
- Defaults loaded if checksum fails
- Memory map specification to be determined by processor

9.11.2 Configuration Checksum

REQ-9112 [ASIL-D]

CRC-16 protection

- Verified at every power-on
- Load defaults and set DTC if checksum fails

9.11.3 Factory Default Restore

REQ-9113 [ASIL-C]

Triggered via:

- CAN command
- EEPROM checksum failure
- Version mismatch

Procedure:

- Write defaults to RAM
- Verify
- Calculate checksum
- Write EEPROM
- Verify
- Log event

9.12 Calibration Procedure

9.12.1 Calibration Steps

REQ-9121 [ASIL-QM]

Recommended Calibration Steps:

- Current-to-Torque Constant (Section 9.5.1)
- Throttle Response Curves (Section 9.1)
- Temperature Setpoints (Section 9.2)
- Traction Control (Section 9.3)
- Sensor Validation Thresholds (Section 9.6.1)

APPENDIX A: Power Up System Tests and Precharge Monitoring Tests

REQ-A01 [ASIL-D]

- **Activities in Power On System Test:**
  - ADC channel validation
  - Watchdog check
  - CAN bus initialization
  - Memory integrity checks
  - Sensor voltage range verification
  - Configuration parameter load from EEPROM and verified.
  - CAN messages all accounted for
  - All contactors are open.
  - Isolation monitoring

REQ-A02 [ASIL-D]

- **Activities in Precharge System Test:**
  - Voltage and current values received from transducer
  - Voltage and current values received from BMS
  - Temperature option: aux temperature input to monitor precharge resistor temperature.
  - Timing option: (TBD) to prevent overheating resistor.
  - Isolation monitor changes do not leave safe range.

APPENDIX B: Calibration

REQ-B01 [ASIL-QM] *(Quality Management - not safety-critical)*

Recommended Calibration Steps:

1. **Current-to-Torque Constant (Section 9.5.1):**
   - Drive vehicle at various throttle positions
   - Log throttle %, actual torque %, actual current
   - Calculate: A/% = actualCurrent / actualTorque
   - Use average value across operating range
2. **Throttle Response Curves (Section 9.1):**
   - Test drive with various exponents (0.5, 0.7, 1.0, 1.5)
   - Driver selects preferred response
   - Or create custom 16×16 map for advanced tuning
3. **Temperature Setpoints (Section 9.2):**
   - Monitor component temperatures during normal operation
   - Set fan thresholds 10-15°C below maximum rated temperature
   - Verify adequate cooling under sustained load
4. **Traction Control (Section 9.3):**
   - Test on low-traction surface (wet, gravel)
   - Adjust Sx/Sy until slip reliably detected
   - Tune torque reduction until wheel spin minimized
5. **Sensor Validation Thresholds (Section 9.6.1):**
   - Generally use defaults
   - If false faults occur: widen tolerances slightly
   - If failures not detected: tighten tolerances

DOCUMENT END