Vehicle Control Unit Requirements

for electric drive system

Requirements & Best Practice

draft 006

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

Vehicle Control Unit (VCU) System Requirements

Compliant Design conforming to component standards

Document Version: 006 DRAFT
Date: 2025-10-17

Reference Documents:

- VCU CAN Protocol Specification (Spreadsheet)
- ZEPS Process for Warning and Shut-down levels

Information in this document was supplemented with research aided with AI. All information should be verified before use, and not assumed to be factual

Most motor and inverter vendors avoid offering VCUs because a VCU sits at the vehicle level, requiring complex integration, functional safety (ISO 26262), and regulatory compliance (ISO 6469, 21434, etc.). Providing one exposes the supplier to major liability for vehicle safety and demands extensive customization, validation, and support for every unique system configuration. In contrast, motors and inverters can be sold as standalone components with far less legal and engineering overhead, so most companies leave vehicle-level control to OEMs or specialized integrators.

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

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

VCU-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 Design Process

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

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

Safety Requirement	Standard(s)	Notes
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

---

2. DIGITAL OUTPUTS

All outputs source current to optocouplers unless specified as MOSFET sink. Default state is OFF unless noted.

2.1 Indicator Outputs (Optocoupler Source)

2.1.1 Ready Light (OUT_READY)

VCU-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)

VCU-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)

VCU-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)

VCU-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)

VCU-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)

VCU-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)

VCU-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)

VCU-REQ-017 [ASIL-A]

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

2.1.9 Reduced Braking Performance Indicator

VCU-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, ...)

VCU-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)

VCU-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)

VCU-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)

VCU-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)

VCU-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)

VCU-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)

VCU-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 Rollaway Alarm (OUT_ROLLAWAY)

VCU-REQ-027 [ASIL-B]

- **State HIGH:** Gear selector in NEUTRAL AND no brake applied
- **State LOW:** Gear not in neutral OR brake applied

2.3 Regulated 5V Outputs

2.3.1 Hardwire Throttle Enable

VCU-REQ-028 [ASIL-D]

- **State HIGH:** Complete (closed) circuit to throttle pedal power 5V
- **State LOW:** Open circuit to throttle pedal power 5V (foot brake applied)

2.3.2 Sensor Power

VCU-REQ-029 [ASIL-C]

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

---

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)

VCU-REQ-030 [ASIL-D]

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

3.1.2 Brake Pedal Applied (IN_BRAKE_PEDAL)

VCU-REQ-031 [ASIL-D]

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

3.1.3 Brake Pedal Released (IN_BRAKE_RELEASED)

VCU-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)

VCU-REQ-033 [ASIL-C]

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

3.1.5 Auxiliary Brake Applied (IN_AUX_BRAKE)

VCU-REQ-034 [ASIL-C]

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

3.1.6 Turtle Mode Toggle (IN_TURTLE_TOGGLE)

VCU-REQ-035 [ASIL-A]

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

3.1.7 Override Mode (IN_OVERRIDE)

VCU-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)

VCU-REQ-037 [ASIL-D]

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

3.1.9 ABS Active (IN_ABS_ACTIVE)

VCU-REQ-038 [ASIL-D]

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

3.1.10 Tow Mode (IN_TOW_MODE)

VCU-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)

VCU-REQ-040 [ASIL-C]

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

3.2.2 Neutral Request (IN_SHIFT_NEUTRAL)

VCU-REQ-041 [ASIL-C]

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

3.2.3 Reverse Request (IN_SHIFT_REV)

VCU-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)

VCU-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)

VCU-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)

VCU-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

VCU-REQ-050 [ASIL-D]

- **Description:** VCU powered down
- **Outputs:** All outputs LOW
- **Entry:** Power removed or watchdog reset

4.1.2 STARTUP

VCU-REQ-051 [ASIL-D]

- **Description:** System initialization and self-test
- **Duration:** 2-5 seconds
- **Outputs:** All outputs disabled

See Appendix 1 for system tests.

4.1.3 STANDBY

VCU-REQ-052 [ASIL-C]

- **Description:** PARKED master switch off
- **Outputs:** All outputs disabled
- **Activities:** Monitor inputs, faults

4.1.4 READY

VCU-REQ-053 [ASIL-D]

- **Description:** Normal operation, drive system functional
- **Outputs:** OUT_READY = HIGH, MAIN RELAY, ACC
- **Activities:**
  - Throttle input processing
  - Torque command generation
  - All safety checks active
  - Auxiliary systems operational

4.1.5 FAULT

VCU-REQ-054 [ASIL-D]

- **Description:** Throttle sensor validation failure
- **Outputs:** OUT_READY = LOW, OUT_MIL = HIGH
- **Torque:** Forced to 0%
- **Activities:**
  - Attempting automatic recovery
  - Logging fault events (*SEE LOGGING - Section TBD*)
  - Monitoring for valid sensor data

4.1.6 EMERGENCY_STOP

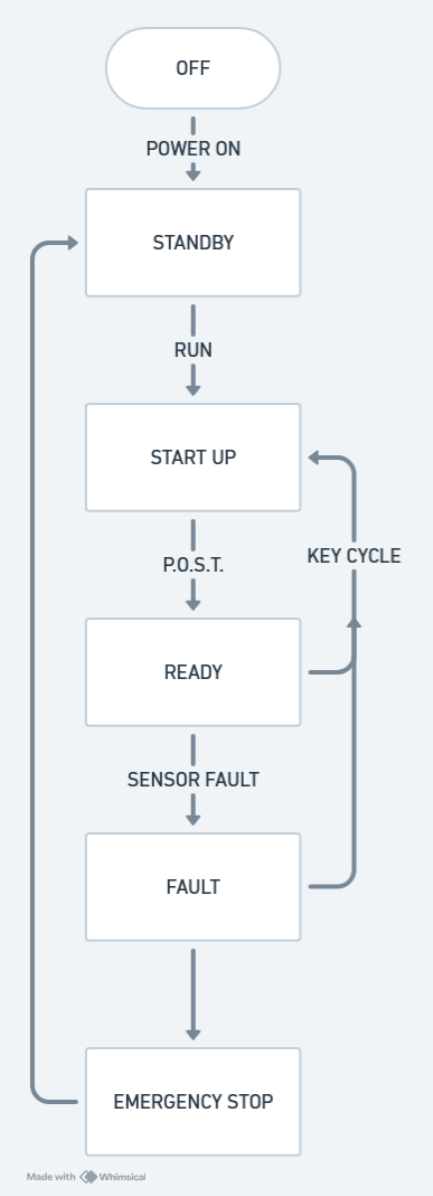
VCU-REQ-055 [ASIL-D]

- **Description:** Critical fault, manual reset required
- **Outputs:** OUT_READY = LOW, OUT_MIL = HIGH, OUT_MAIN = LOW
- **Torque:** All drive functions disabled
- **Activities:**
  - Logging critical fault
  - Waiting for manual reset (key cycle)

4.1.7 TOW_MODE

VCU-REQ-056 [ASIL-A]

- **Description:** Vehicle being moved with external power
- **Outputs:** OUT_ACCESSORY = HIGH, OUT_MAIN = LOW, ready light 2Hz flash
- **Activities:**
  - Accessory power only
  - Drive system disabled
  - Bypasses fault checks



4.2 State Transition Conditions

4.2.1 OFF → STANDBY

VCU-REQ-060 [ASIL-D]

- **Trigger:** POWER ON
- **Requirements:**
  - Power On System Test pass
  - Power supply stable
  - BMS CAN responding

4.2.2 STANDBY → STARTUP

VCU-REQ-061 [ASIL-D]

- **Trigger:** IN_RUN goes HIGH (key ON)
- **Requirements:** Power supply stable
- **Activities:**
    - Precharge process (Section 6.8)

4.2.3 STARTUP → READY

VCU-REQ-062 [ASIL-D]

- **Requirements (all must be true):**
    - Precharge complete
    - Both throttle sensors reading 0.5V-4.5V
    - Sensors agree within 10% (0.5V)
    - Motor controller CAN responding
    - BMS CAN responding
    - Throttle position < deadband (2% per Section 9.6.1)
    - No faults detected

4.2.4 READY → FAULT

VCU-REQ-063 [ASIL-D]

- **Trigger (any):**
    - Throttle sensors disagree > 10% (0.5V per Section 9.6.1)
    - Sensor voltage < 0.5V or > 4.5V (rail voltage)
    - Sensor gradient exceeds physical limit (1.33% per 2ms per Section 9.6.1)
    - Sensor stuck (no variance when throttle > 5% for 500ms on hi-res inputs)
- **Transition:** Immediate (no delay)

4.2.5 FAULT → READY

VCU-REQ-064 [ASIL-D]

- **Requirements (all must be true):**
    - 500ms continuous valid sensor readings (per Section 9.6.2)
    - Sensors agree within 10% (per Section 9.6.1)

- Throttle position < 2% (deadband per Section 9.6.1)
- No other faults active

4.2.6 Any State → EMERGENCY_STOP

VCU-REQ-065 [ASIL-D]

- **Trigger (any):**
  - Motor controller CAN timeout (>100ms per Section 9.7.1)
  - BMS CAN timeout (>200ms per Section 9.7.1) AND IN_OVERRIDE = LOW
  - System voltage < 9V (12V system fault)
  - Watchdog timeout (100ms per Section 9.9.1)
  - Startup self-test failure
  - Torque tracking error > 25% for >100ms

4.2.7 EMERGENCY_STOP → STARTUP

VCU-REQ-066 [ASIL-D]

- **Trigger:** IN_RUN toggled LOW then HIGH (master switch on)
- **Requirements:** Power cycle or master switch reset

5. THROTTLE INPUT PROCESSING (HIGHEST PRIORITY)

5.1 Hardware Configuration

5.1.1 Dual Sensor Architecture

VCU-REQ-070 [ASIL-D]

- Two independent analog throttle position sensors (TPS1, TPS2)
- Voltage range: 0.5V to 4.5V operating (10% margin from rails)
- ADC resolution: Minimum 10-bit (1024 steps = 0.49% resolution)
- Sample rate: 500 Hz (2ms loop time)
- Electrical isolation: RC filters on each input (100Ω + 100nF minimum)

5.1.2 Processing Priority

VCU-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

VCU-REQ-072 [ASIL-D]

- **Maximum deviation:** 10% of full scale (0.5V on 5V scale per Section 9.6.1)
- **Action if violated:** Transition to FAULT state immediately
- **Purpose:** Detect wiring fault, sensor failure, or electrical interference

5.2.2 Voltage Range Check

VCU-REQ-073 [ASIL-D]

- **Valid range:** 0.5V to 4.5V
- **Rail voltage detection:** Reading < 0.5V or > 4.5V indicates:
    - Wire break (open circuit)
    - Short circuit to ground or Vcc
    - Sensor power supply failure
- **Action if violated:** Transition to FAULT state immediately
- **EXCEPTION**: Hardwire throttle interlock (Section 5.5)

5.2.3 Gradient Plausibility Check (Physical Limit)

VCU-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

VCU-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 FAULT state
- **Purpose:** Detect frozen sensor or broken signal path

5.3 Signal Processing

5.3.1 Noise Filtering

VCU-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

VCU-REQ-077 [ASIL-D]

- **Calculation:** Depended on throttle type:
  - Ratiometric sensors: throttlePosition = (TPS1_filtered + TPS2_filtered) / 2
  - Opposing sensors: throttlePosition = (TPS1_filtered + (100 - TPS2_filtered)) / 2
  - Asymmetric sensors: throttlePosition = (TPS1_normalized + TPS2_normalized) / 2
- **Output range:** 0% to 100%

5.3.3 Deadband Application

VCU-REQ-078 [ASIL-C]

- **Threshold:** 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

VCU-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

VCU-REQ-080 [ASIL-D]

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

5.5 Hardwire Throttle Interlock

VCU-REQ-081 [ASIL-D]

An explanation of how the "hardwire" throttle disable system works:

1. When the brake is applied, the hardware brake override circuit cuts power to the **Hardwire Throttle Enable** (OUT per Section 2.3.1). This causes the throttle sensor input to drop to zero or an invalid level, which is expected behavior, NOT a sensor fault.
2. The VCU firmware recognizes this as a controlled power cutoff event, entering a diagnostic mode that temporarily ignores throttle signal faults caused by the power loss.
3. On brake release, the power to the throttle sensor is restored; the throttle sensor signal may be unstable initially.
4. The VCU waits for the throttle input to return to “deadband” and other test parameters pass before it processes new throttle commands, preventing immediate acceleration from a held throttle position.

---

6. TORQUE CONTROL AND SAFETY FUNCTIONS

6.1 Torque Request Generation

6.1.1 Throttle-to-Torque Mapping

VCU-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

VCU-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

VCU-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:

- If no BMS message (per Section 9.7.1):
    - Log timeout event
    - Turn on MIL

6.2.2 DCL Limiting

VCU-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).
- If IN_OVERRIDE = LOW: transition to EMERGENCY_STOP

6.2.3 Motor Controller Feedback

VCU-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

VCU-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

VCU-REQ-096 [ASIL-C]

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

- Disable all regenerative braking
- Route brake pedal to friction brakes only
- Turn on BRAKE PERFORMANCE REDUCED output (OUT per Section 2.1.9) (FMVSS 105 requirement)

6.2.6 Temperature-Based Derating

VCU-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

VCU-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: unintendedMotionDetected = TRUE (see CAN protocol)
- Force torqueRequest = 0%
- Log safety event
- Turn on OUT_ROLLAWAY (per Section 2.2.8)
    - NOTE: OUT_ROLLAWAY is also applied in 6.6.1. When in Neutral, 6.6.1 applies. When in a drive gear 6.3.1 applies.

Clear Condition:

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

6.3.2 Brake Pedal Override (Highest Priority)

VCU-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

VCU-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

VCU-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

VCU-REQ-104 [ASIL-D]

Park/Neutral:

IF (Park brake ON):

- 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 directional fault
- Display: "Drivetrain Error"

// Prevents motor fighting forward momentum

6.4 Tow Mode

6.4.1 Activation

VCU-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

6.4.2 Behavior

VCU-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)

VCU-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)

VCU-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

VCU-REQ-109 [ASIL-B]

IF (gearMode = NEUTRAL) AND (ALL brake signals LOW):
- OUT_ROLLAWAY = HIGH

ELSE:
- OUT_ROLLAWAY = LOW

Don't forget about the other thing that turns this on

6.7 Cooling Fan Control

6.7.1 Algorithm (per fan output)

VCU-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:
  - C1 = 70°C default for motor winding (Section 9.2.1)
  - C2 = 65°C default for inverter (Section 9.2.1)
- 2°C hysteresis prevents rapid cycling

6.7.2 Temperature Sources

VCU-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 Sequence

6.8.1 Startup Sequence

VCU-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

- Verify contactor position
- Read voltages from:
  - Voltage transducer (see CAN Protocol doc)
  - 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

VCU-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
- Log data and results to CAN

6.9 Override Mode

6.9.1 Function

VCU-REQ-114 [ASIL-B]

IF (IN_OVERRIDE = HIGH):

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

VCU-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

VCU-REQ-116 [ASIL-B]

Detect wheel slip when:

- deltaRPM > Sx over time period < Sy

Where:

- deltaRPM = change in motor RPM
- Sx = configurable RPM threshold (default 500 RPM per Section 9.3.1)
- Sy = configurable time window (default 100ms per Section 9.3.2)

6.10.2 Slip Response

VCU-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)

VCU-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)

VCU-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)

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

VCU-REQ-130 [ASIL-D]

See document: *ZEPS Process for Warning and Shut-down levels V1.0 or newer*

- Clear safety reactions for each fault bit,
- Demonstrated diagnostic coverage and fault detection effectiveness,
- Systematic verification and traceability,
- Reliable safe state transitions beyond logging.

---

9. CONFIGURATION AND CALIBRATION PARAMETERS

9.1 Torque Mapping Configuration

9.1.1 Response Curve Exponents

VCU-REQ-140 [ASIL-C]

Normal Mode Exponent:

- Default: 1.0 (linear)
- Range: 0.5 to 2.0
- Units: dimensionless
- Description: throttlePosition raised to this power
  - <1.0 = gentler initial response
  - 1.0 = linear
  - ***>1.0 = aggressive initial response (original stated "1.0")***

Turtle 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)

VCU-REQ-141 [ASIL-A]

The following parameters affect vehicle performance but not safety functions:

Parameter	Reference	Default	Valid Range	Units
Normal mode response	6.1.1	1.0	***0.5 to 2.0 (original stated "1.0")***	dimensionless
Turtle mode response	6.1.1	0.7	0.3 to 0.9	dimensionless
Torque ramp-up rate	6.1.2	200%/s	100 to 400%/s	%/second
Torque ramp-down rate	6.1.2	400%/s	200 to 800%/s	%/second
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

VCU-REQ-142 [ASIL-A]

Fan 1 Setpoint (C1):

- Default: 70°C
- Range: 40°C to 90°C
- Description: Motor winding temperature threshold
- Reference: Section 6.7.1

Fan 2 Setpoint (C2):

- Default: 65°C
- Range: 40°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)

VCU-REQ-143 [ASIL-B]

Motor RPM Delta:

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

9.3.2 Slip Detection Time Window (Sy)

VCU-REQ-144 [ASIL-B]

Time Period:

- Default: 100 ms
- Range: 50 to 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

VCU-REQ-145 [ASIL-B]

Torque Reduction:

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

Hold Duration:

- Default: 500 ms
- Range: 250 to 2000 ms
- Description: Time to hold reduced torque before restoring
- Reference: Section 6.10.2

Restore Ramp Rate:

- Default: 1 second (0 → 100%)
- Range: 0.5 to 3 seconds
- Description: Time to gradually restore torque after slip event
- Reference: Section 6.10.2

9.4 Hill Hold Parameters

9.4.1 Activation Threshold (Qx)

VCU-REQ-146 [ASIL-B]

Torque Threshold:

- Default: 15%
- Range: 5% to 30%
- Description: Torque level at which hill hold releases
- Reference: Section 6.5.2

9.4.2 Activation Conditions

VCU-REQ-147 [ASIL-B]

RPM Threshold:

- Default: 2 RPM (nearly stopped)
- Range: 0 to 10 RPM
- Description: Maximum vehicle speed for hill hold activation
- Reference: Section 6.5.1

Brake Required:

- Fixed: IN_BRAKE_PEDAL must be HIGH
- Reference: Section 6.5.1

9.5 Current Limiting Parameters

9.5.1 Current-to-Torque Conversion

VCU-REQ-148 [ASIL-D]

Calibration Constant:

- Default: 5.5 A per 1% torque (550A nominal / 100%)
- Range: 3.0 to 10.0 A/%
- Description: System-specific current draw per torque percent
- **Must be calibrated** for actual motor/inverter combination
- Reference: Section 6.2.2, Appendix 2 Calibration Step 1

9.5.2 Soft Limiting Thresholds

VCU-REQ-149 [ASIL-C]

Some values have warning levels that will trigger reduced performance (turtle mode). These values are outlined in the document “ZEPS Process for Warning and Shut-down levels”

9.5.3 BMS Timeout Defaults

VCU-REQ-150 [ASIL-D]

Timeout to disable. If BMS CAN is not received for more than the specified time, an emergency stop will occur.

9.6 Safety Interlock Parameters

9.6.1 Throttle Sensor Validation

VCU-REQ-151 [ASIL-D]

Correlation Tolerance:

- Default: 10% (0.5V on 5V scale)
- Range: 5% to 15%
- Description: Maximum allowed difference between TPS1 and TPS2
- Reference: Section 5.2.1, 4.2.3, 4.2.4, 4.2.5

Gradient Limit:

- Default: 1.33% per 2ms (100% in 150ms)
- Range: 0.5% to 3.0% per 2ms
- Description: Maximum allowed throttle change per sample
- Reference: Section 5.2.3, 4.2.4

Stuck Detection Variance:

- Default: 0.2% over 100ms

- Range: 0.1% to 1.0%
- Description: Minimum sensor movement required to confirm not stuck
- Reference: Section 5.2.4

Deadband:

- Default: 2%
- Range: 1% to 5%
- Description: Throttle position below which output is zero
- Reference: Section 5.3.3, 4.2.3, 4.2.5

9.6.2 Sensor Fault Recovery Time

VCU-REQ-152 [ASIL-D]

Validation Period:

- Default: 500 ms
- Range: 200 to 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

VCU-REQ-153 [ASIL-D]

RPM Threshold:

- Default: 100 RPM
- Range: 50 to 500 RPM
- Description: Minimum vehicle speed for unintended motion check
- Reference: Section 6.3.1

Torque Threshold:

- Default: 10%
- Range: 5% to 20%
- Description: Minimum torque to consider "significant"
- Reference: Section 6.3.1

9.7 CAN Bus Parameters

9.7.1 Timeout Thresholds

VCU-REQ-154 [ASIL-D]

Motor Controller Timeout:

- Default: 100 ms
- Range: 50 to 500 ms
- Description: Max time without motor controller message before EMERGENCY_STOP
- Reference: Section 4.2.6

BMS Timeout:

- After specified time, system will go to emergency stop.
- Range: 100 to 1000 ms
- Description: Max time without BMS message before action
- Action depends on IN_OVERRIDE state
- Reference: Section 4.2.6, 6.2.1

9.8 Precharge Parameters

9.8.1 Voltage Matching Tolerance

VCU-REQ-155 [ASIL-D]

Precharge Threshold:

- Default: 5% voltage difference
- Range: 2% to 10%
- Description: Max difference between capacitor and battery voltage
- Reference: Section 6.8.1 Step 3

Precharge Timeout:

- Default: 10 seconds
- Range: 5 to 30 seconds
- Description: Max time allowed for precharge completion
- Reference: Section 6.8.1 Step 3, 6.8.2

9.9 Watchdog Parameters

9.9.1 Watchdog Timeout

VCU-REQ-156 [ASIL-D]

Timeout Period:

- Default: 100 ms
- Range: 50 to 500 ms
- Description: Max time between watchdog kicks before reset
- Reference: Section 4.2.6

Kick Frequency:

- Fixed: Every control loop (2ms)
- Must be <50% of timeout period

9.10 Override Mode Parameters

9.10.1 Override Timer

VCU-REQ-157 [ASIL-B]

Maximum Override Duration:

- Default: 15 seconds (momentary switch)
- Range: 5 to 60 seconds
- Description: Time allowed for override mode before timeout
- Reference: Section 6.9.2

9.10.2 Override Performance Limits

VCU-REQ-158 [ASIL-B]

Torque Limit in Override:

- Same as turtle mode
- Reference: Section 6.9.1

9.11 Configuration Mangement

9.11.1 EEPROM Memory Map

VCU-REQ-159 [ASIL-D]

Safety relevant memory

- contents will be verified by a checksum on startup.
- If checksum fails, defaults will be used.
- Default values will be written into the main program
- When hardware is determined, further security options will be considered.

9.11.2 Configuration Checksum

VCU-REQ-160 [ASIL-D]

CRC-16 Protection: (bare minimum)

- Calculated over all calibration parameters
- Verified at every power-on
- If checksum fails: Load factory defaults, set DTC

9.11.3 Factory Default Restore

VCU-REQ-161 [ASIL-C]

Trigger Conditions:

- CAN command from service tool
- EEPROM checksum failure
- Configuration version mismatch

Procedure:

1. Write factory default values to RAM
2. Verify defaults are sensible
3. Calculate checksum
4. Write to EEPROM
5. Verify write successful
6. Log configuration reset event

9.12 Calibration Procedure

VCU-REQ-162 [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

APPENDIX 1: Power Up System Tests and Precharge Monitoring Tests

VCU-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

VCU-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

APPENDIX 2: Calibration

VCU-REQ-A02 [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