Automotive and Aerospace Systems

- Networked control.
- Vehicular networks:
  - CAN.
  - TTP, FlexRay, etc.
- Safety and security.

Marilyn Wolf
"Computers as Components, 4e"
Chapter 9

Networked control

- Computer networks that perform real-time control functions.
  - Allows more computing power to be applied than is available from a single CPU.
  - Allows processors to be physically near the devices they control.
- Electronic control unit (ECU) is a digital unit in a car.
- Line replaceable unit (LRU) is a module in an airplane avionics system.

Vehicles as networks

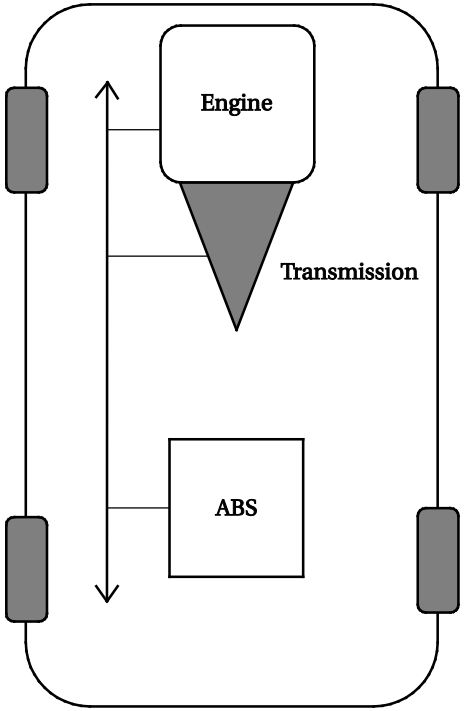
- 1/3 of cost of car/airplane is electronics/avionics.
- Modern cars may have 100+ processors and operate with 100 million lines of code.
- Network applications:
  - Vehicle control.
  - Instrumentation.
  - Communication.
  - Passenger entertainment systems.

Example automotive processors

- Infineon XC2200 body control processor:
  - 16/32 bit processor.
  - SRAM and EEPROM.
  - Analog/digital converter.
  - Pulse width modulator.
  - Serial channels.
  - Light drivers.
  - Network connections.
- Freescale MPC5767R for powertrain systems.
- Dual-processor Power Architecture CPUs, including vector processors.
- 16K data and instruction caches.
- Time processing unit used to generate and read waveforms.
- CAN, Lin, FlexRay interfaces.

Automobile network

- Engine provides power to drive the wheels via the transmission.
- Transmission adjusts gearing based on operating characteristics.
- ABS controls brakes.

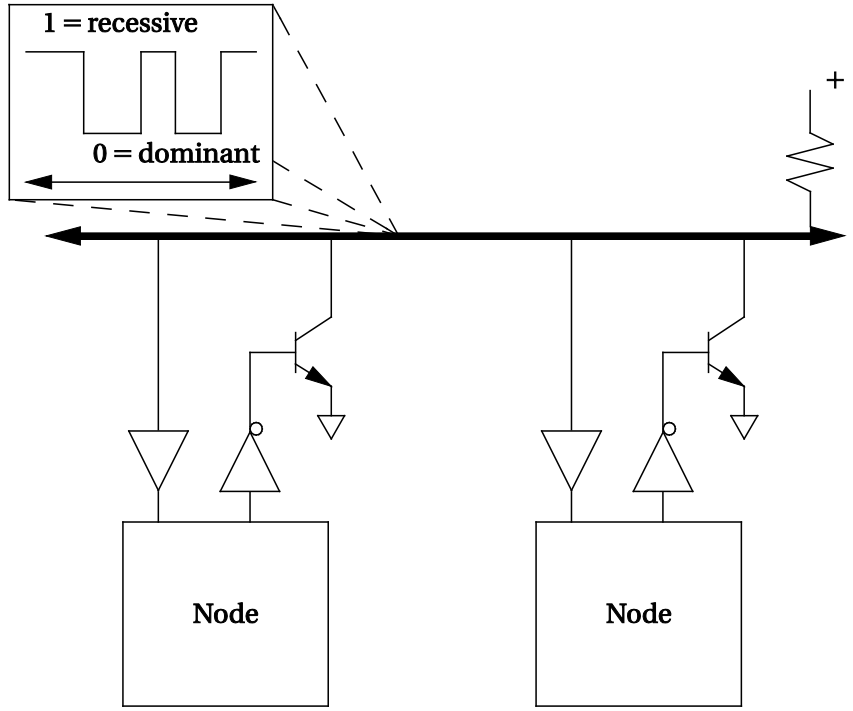


Avionics

- Avionics design must be certified.
- Architectural evolution:
  - Modular architecture has a separate LRU for each function (artificial horizon, engine control, etc.)
  - Federated network has networks grouped by function (flight controls, navigation, etc.).
  - Genesis Platform defines virtual avionics system that is mapped onto a physical network.

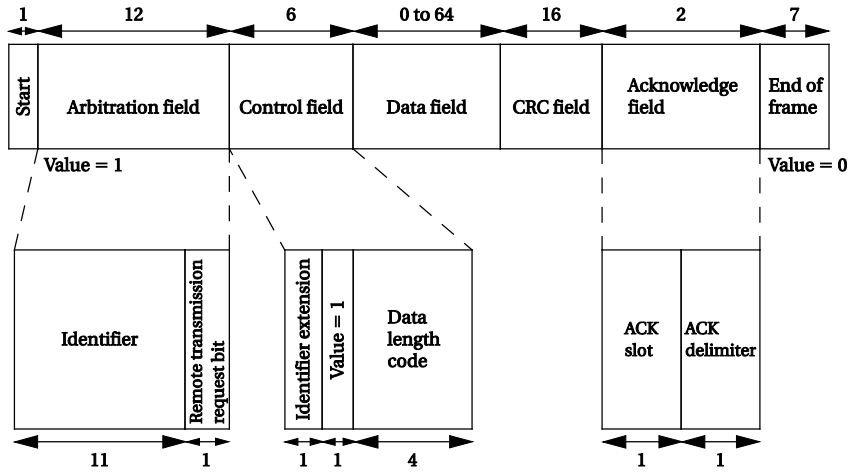
CAN bus

- First used in 1991.
- Serial bus, 1 Mb/sec up to 40 m.
- Synchronous bus.
- Logic 0 dominates logic 1 on bus.
- Arbitrated with CSMA/AMP:
  - Arbitration on message priority.



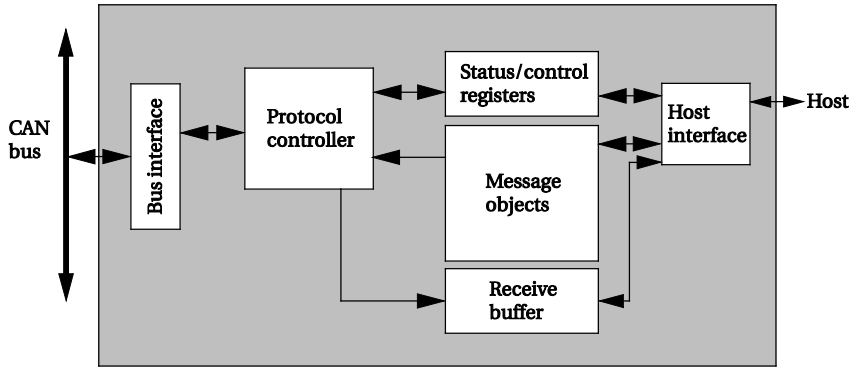
CAN data frame

- 11 bit destination address.
- RTR bit determines read/write from/to destination.
- Any node can detect bus error, interrupt packet for retransmission.



CAN controller

- Controller implements physical and data link layers.
- No network layer needed---bus provides end-to-end connections.



Other vehicle busses

- Time-triggered architecture (TTA) assigns communications to time slots.
- FlexRay is next generation:
  - Time triggered protocol.
  - 10 Mb/s.
- Local Interconnect Network (LIN) connects devices in a small area (e.g., door).
- Passenger entertainment networks:
  - Bluetooth.
  - Media Oriented Systems Transport (MOST).

Safety and security

- Vehicles are safety-critical systems.
- Threat models:
  - Maintenance technicians may introduce problems either maliciously or accidentally.
  - Component suppliers may supply components that don’t work with the system or include malware.
  - Passengers may introduce malware either maliciously or accidentally.
  - Passers-by may connect to vehicle wireless networks.

Car hacking (1)

- UCSD researchers demonstrated a variety of attacks that allowed them to gain complete control of a car.
- Attack vectors:
  - Infecting diagnostic computers used by mechanics.
  - Using a specially-coded CD to load malware onto the CD player.
  - Sending signals over the car's telematics connection.

Car hacking (2)

- CMU researchers demonstrated a takeover of a Jeep Cherokee driven by a journalist.
- Attack vector:
  - Entered car through telematics systems.
  - Entertainment system was then attacked and modified.
  - Car components did not check the validity of software updates.
- Entertainment system was used to send messages over CAN bus to kill engine, disable brakes.

Car crashes

- Oklahoma court ruled that Toyota was liable in a case of unintended acceleration.
  - Electronic throttle control system source code contained 67 functinos with a cyclomatic complexity of over 50; throttle angle function had a cyclomatic complexity of 146.
  - Car's fail-safe capabilities were both inadequate and defective.

Airplane hacking

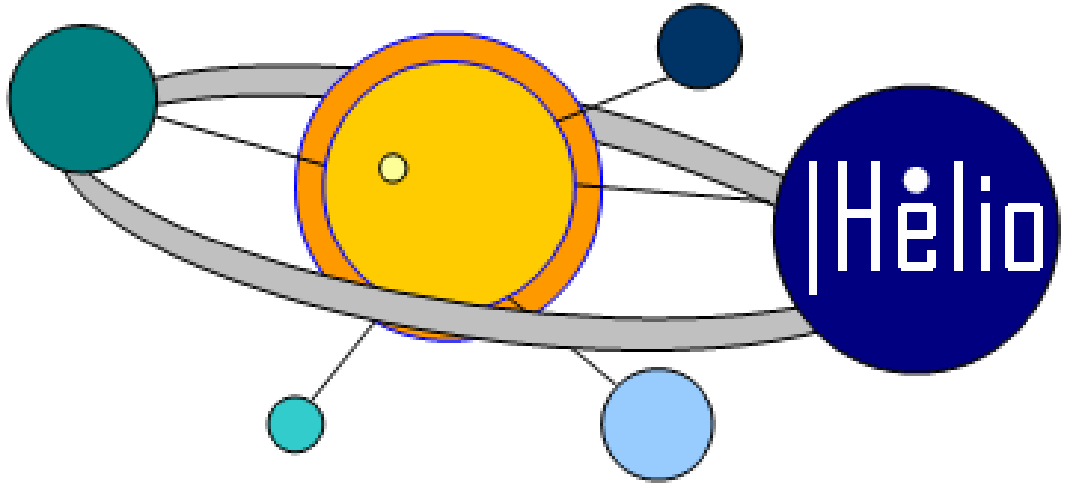
- A computer security researcher was arrested in 2015 on suspicion of having hacked into a Boeing 737 during a flight.
  - Attack vector was through in-flight entertainment system.
  - Allegedly modified code in the Thrust Management Computer.

Software implicated in fatal airplane crash

- Software bugs are suspected to have caused the crash of an Airbus A400M.
  - Software in the ECUS are suspected to have caused three of four engines to shut down during flight.

VW diesel defeat

- VW admitted to installing a defeat of its own software on diesel cars.
  - Defeat enabled strong emissions controls while car was being tested, disabled emissions controls during normal driving.



Link Ltd.

Solar Car CAN Development
Senior Design Project

Mike Cornelison
Beau Eckermann
David Last
Aaron Steiner
Luke Stewart
Brian Whitehousev

Sol of Auburn

- Student built and maintained vehicle
- Runs completely of solar energy
- Races long competitions

Problem Description

- Improve method of communication between subsystems of AU solar car
- Allow driver access to new features such as turn indicators, trip odometer, cruise control, etc.
- Provide driver and chase vehicle (via wireless modem) with real-time system information
- Improve vehicle safety by implementing a “safe mode” for powering down in the event of a system fault
- Reduce size, weight, power consumption

Systems

Motor Controller:

- Powers the motor
- Breaks the vehicle
- Monitors the primary electrical systems

Steering and Throttle:

- Acceleration
- Regenerative breaking
- Turing and breaking signals

Display and Power Controls:

- Speed
- Currents and voltages
- Switch bank

The Design Problem

- Bulky wire harness
  - Adds weight
  - Reliability and packaging problems
  - Noise due to other voltage systems

Solution Idea

Implement a Controller Area Network:

- Connect system devices
  - Motor controller
  - Steering and throttle
  - Display
- CAN Advantages:
  - Fewer wire count
  - Failure detection and safe mode
  - Weight loss
  - Easier installation and maintanance
  - Driver safety

Requirements

- Data handling Speed (1 Mbs)
- Safe Mode for driver safety
- Must run and not exceed 48 watts

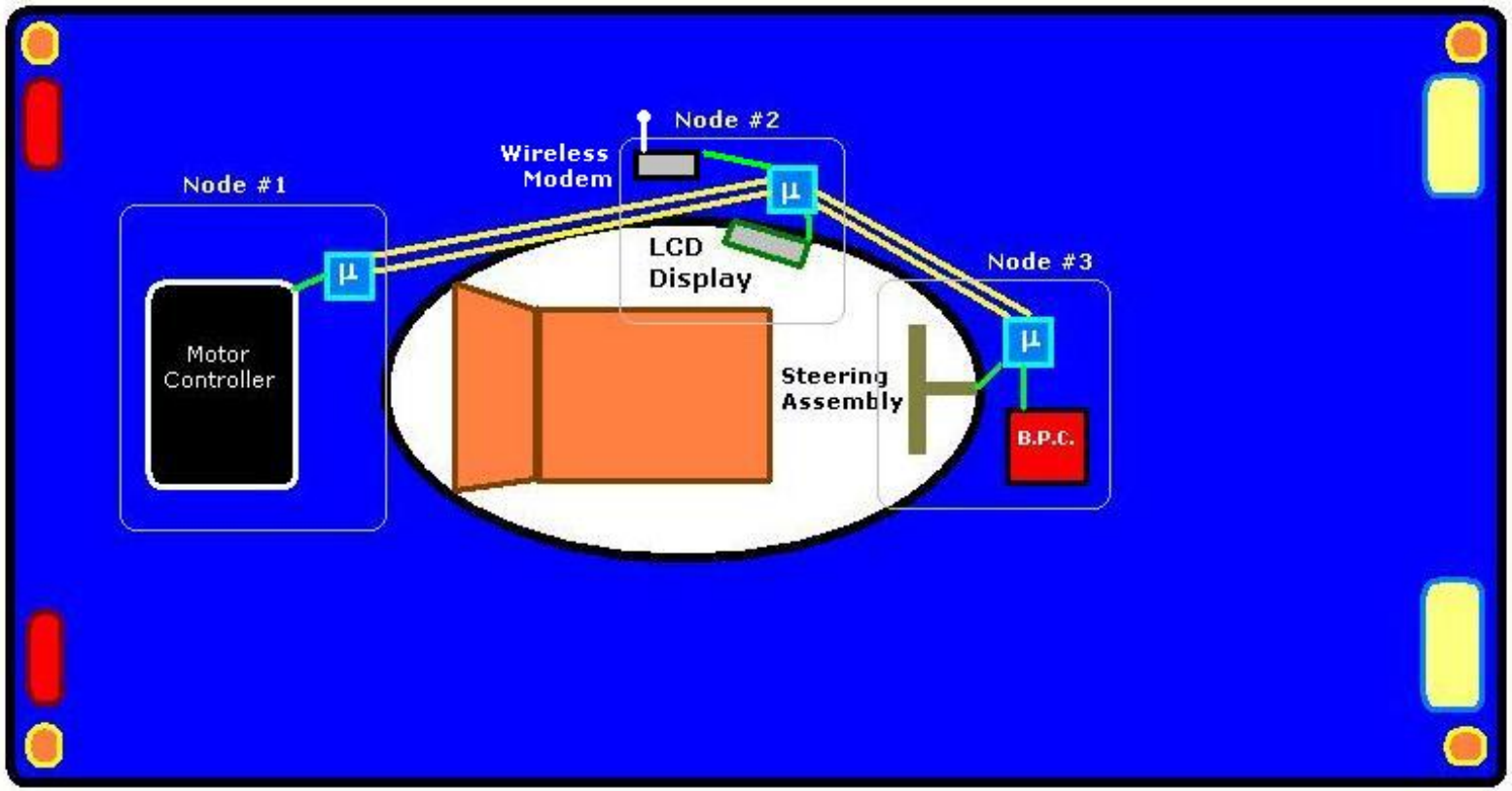
Constraints

- Low current limits
- Low power consumption
- Lightweight
- Functionality
- Cheap

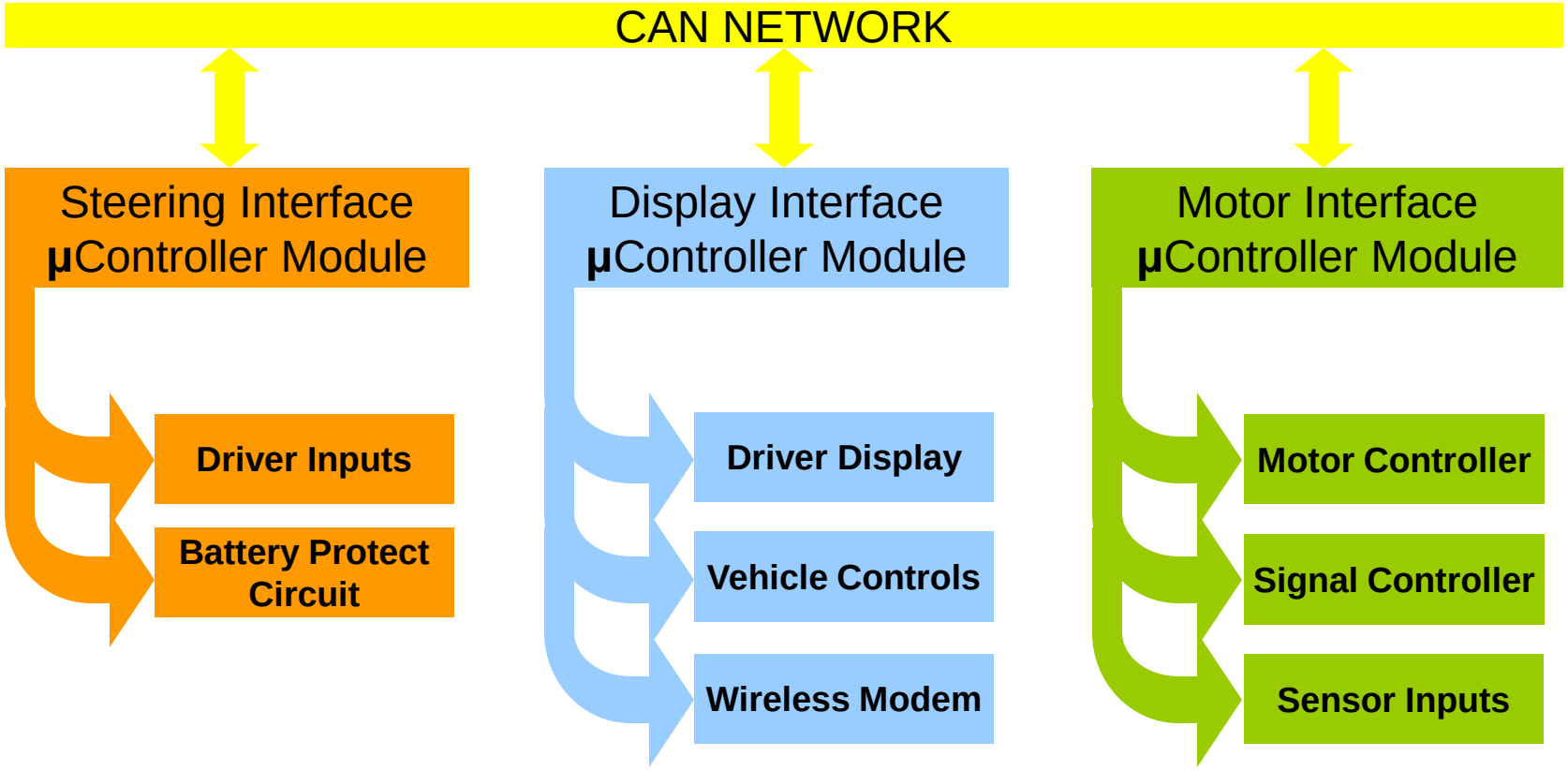
The Approach - Overview

- The Controller Area Network
  - Localized network of independent node devices
    - Most commonly microcontrollers
  - Standardizes communication format, arbitration, and addressing
    - Other network layers (i.e. Physical Layer) can be implemented as the designer sees fit
  - Hardware and Software must be implemented

Overhead Car Diagram



Network Architecture



I/O Summary

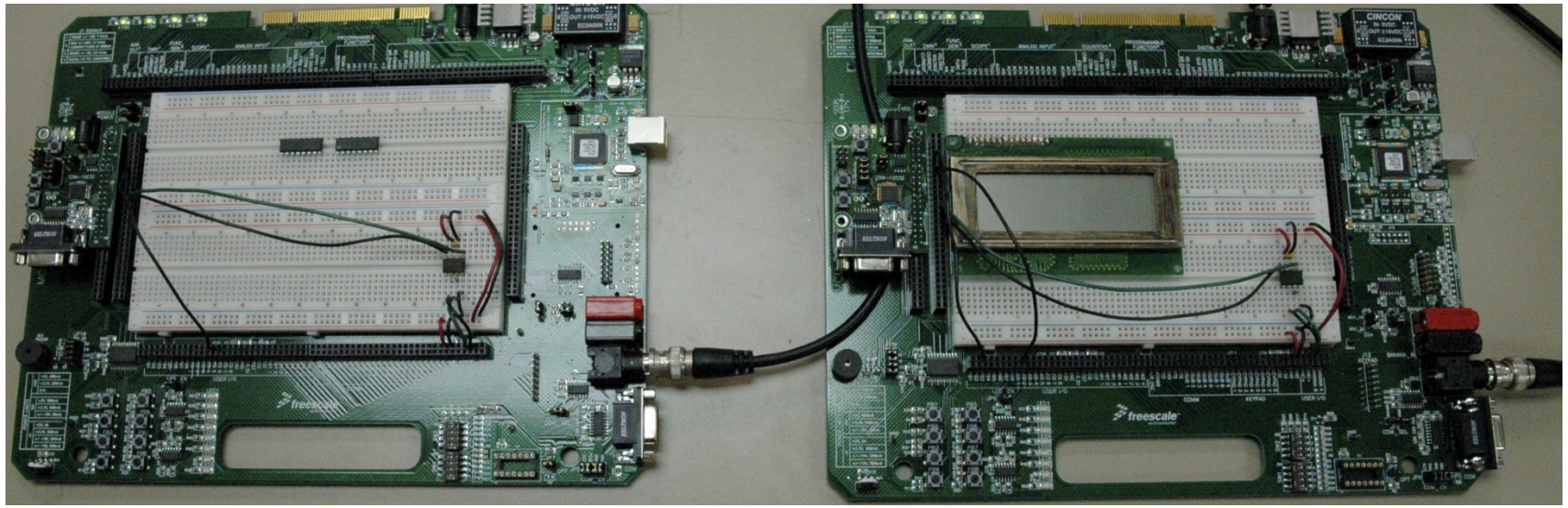
I/O Name	I/O Label	Type	Source No	Source De	Destinatior	Destinatior
Driver Display	display	Digital	Display	-	-	-
Direction Control	dir	Digital	Display	Switch	Motor	Motor Cont
Hazard Lights	hazard	Digital	Display	Switch	Motor	Signal Con
Ignition Control	ignition	Digital	Display	Switch	Motor	Motor Cont
Mph/kph Toggle	mph/kph	Digital	Display	Switch	Display	Internal
Throtle Enable	threnable	Digital	Display	Switch	Motor	Motor Cont
Auxilary Battery Volta	aux_volt	Analog	Motor	Sensor	Display	Display
Break	brake	Digital	Motor	Motor Con	?	?
Main Battery Voltage	main_volt	Analog	Motor	Sensor	Display	Display
Solar Array Current	array_amp	Analog	Motor	Sensor	Display	Display
Solar Array Voltage	array_volt	Analog	Motor	Sensor	Display	Display
Speed Pulse	spdpulse	PWM	Motor	Motor Con	Display	Display
State of Charge	SOC	PWM	Motor	Motor Con	Display	Display
Break Light	brake_light	Digital	Steering	Switch	Motor	Signal Con
Cruise Control -	cc_down	Digital	Steering	Switch	Motor	Internal
Cruise Control +	cc_up	Digital	Steering	Switch	Motor	Internal
Cruise Control Set	cc_set	Digital	Steering	Switch	Motor	Internal
Display Control	disp_toggle	Digital	Steering	Switch	Display	Display
Left Turn Signal	left_turn	Digital	Steering	Switch	Motor	Signal Con
Regen	rgn	Analog	Steering	5K POT	Motor	Motor Cont
Right Turn Signal	right_turn	Digital	Steering	Switch	Motor	Signal Con
Throttle	thr	Analog	Steering	5K POT	Motor	Motor Cont

Hardware

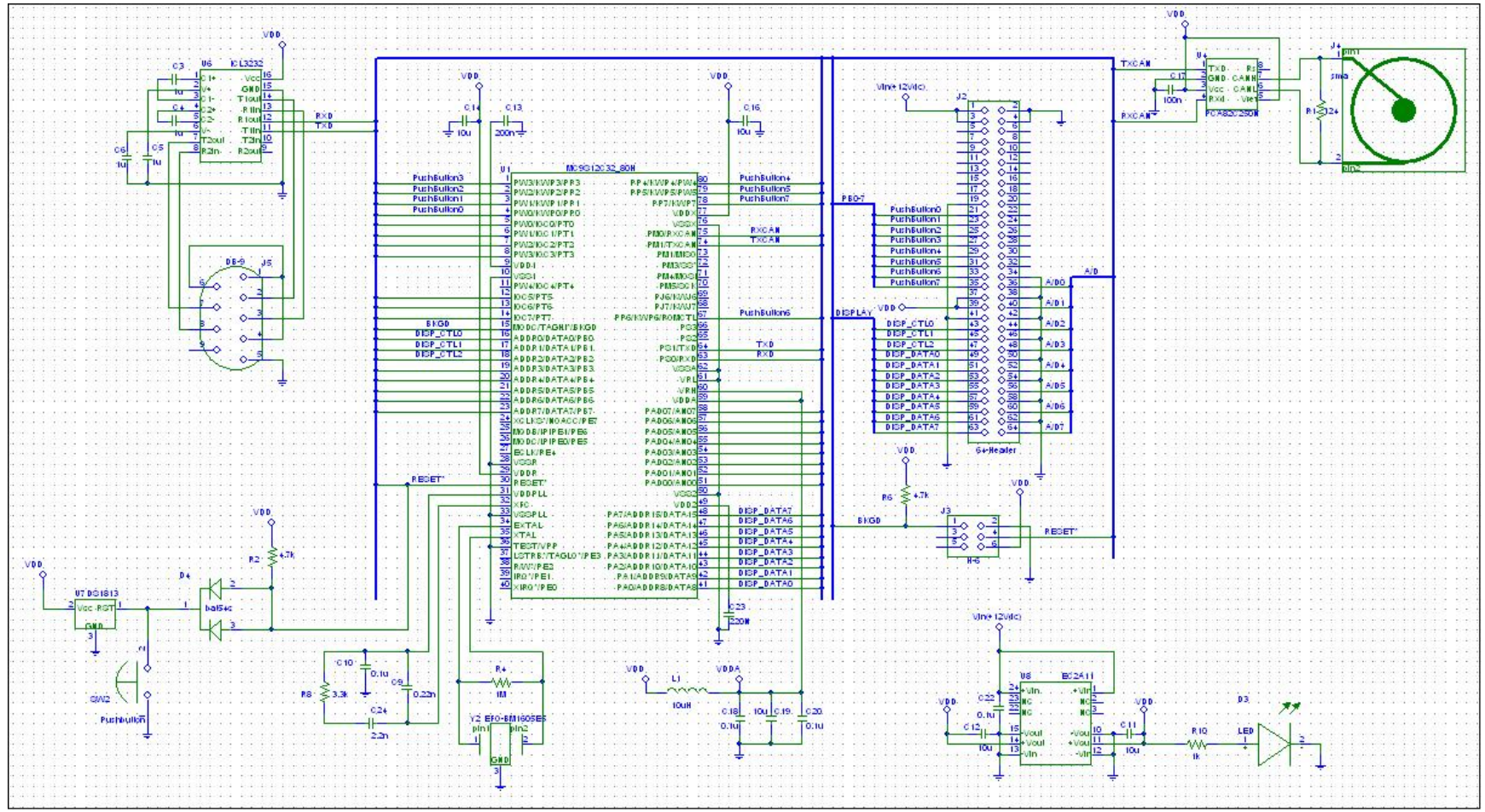
- Freescale's MC9S12C32 microcontroller
  - Versatile microcontroller core with CAN interface
  - Plenty of input and output pins
  - Development hardware (MCU-SDK)
  - CAN Transceiver (Phillips PCA82C250N)

- Three modules throughout the car
  - Steering, Motor and Display Interfaces

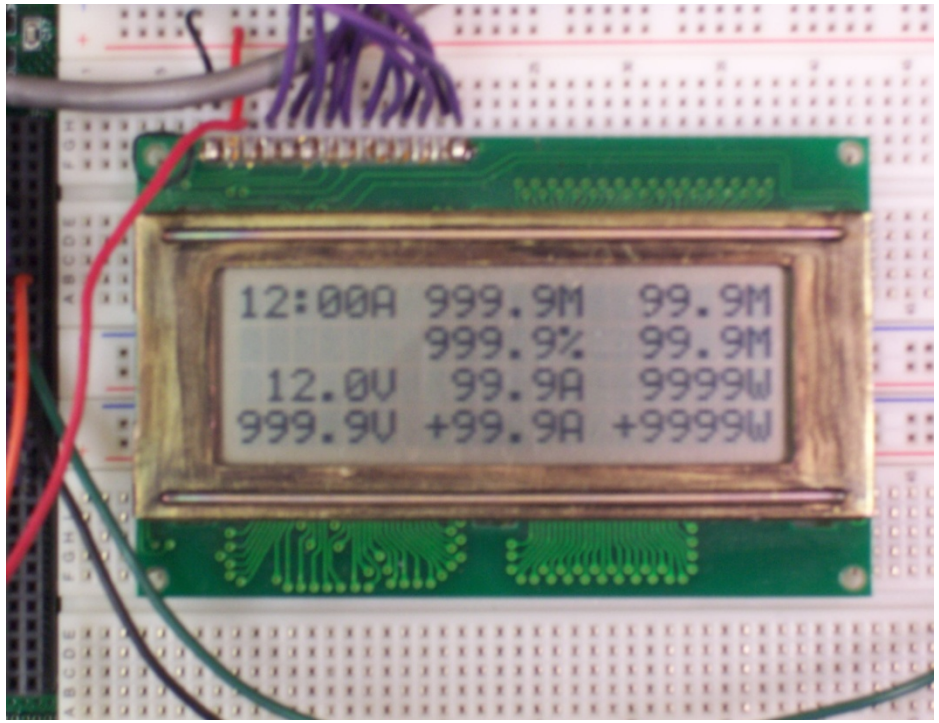
Development setup



Hardware Schematic



Optrex 20x4 LCD display



Software

- CAN communication
- Analog-to-Digital conversion
- Push button interrupts
- RS-232 communication
- Timers
- Display

Steering Interface Module (SIM)

- Collects driver inputs
  - Acceleration, deceleration, brake rate and turn signals
- Analog inputs (ADC)
  - Two potentiometers and one brake rate sensor
- Momentary switches (Interrupts)
  - Cruise control, turn signals, brake pedal, display toggle

Motor Interface Module (MIM)

- Analog outputs
  - Acceleration, deceleration, breaking rate
- Digital outputs
  - Cruise control, turn signals, brake lights
- Pulse width modulated input communicates motor speed and current
- Analog inputs
  - Battery and solar array current, battery voltages

Display Interface Module (DIM)

- Input from other modules
  - Analyzes and outputs information to an LCD display
- Input from bank of eight switches
  - Switches do not yet have a function

Software

- Sends and receives data over the network
- Collects data from car components
  - Decide priority structure of data
- Forces car into shut-down “safe mode” if network connectivity has been lost

Future Work

- Node formation for each subsystem
- CAN message hierarchy
- RS-232 packetization of streaming data
- Safe Mode implementation