ELECTRONIC BYPASS ON COMMERCIAL VEHICLES

TEAM MEMBERS: ANDREW FISHELL, ANDREW OLARIU, JESSE SNYDER, ANTHONY SPAULDING, DAVID ZARAGOZA

MENTORS: JOHN LEWIS AND WILLIAM SHEPHERD

Ira A. Fulton Schools of Engineering
Arizona State University
School of Electrical, Computer and Energy Engineering

PROBLEM STATEMENT

CRITICAL SAFETY FEATURES LIKE ABS AND LIMP-HOME MODE, WHILE ESSENTIAL FOR CIVILIAN USE, CAN HINDER VEHICLE FUNCTIONALITY IN MILITARY SCENARIOS. IN COMBAT ZONES, OPERATORS NEED CONTINUOUS VEHICLE USABILITY REGARDLESS OF ELECTRONIC ERRORS OR DAMAGE. THIS PROJECT AIMS TO BYPASS SUCH SAFETY MECHANISMS IN TOYOTA HILUX VEHICLES TO ENSURE UNINTERRUPTED OPERATION USING CAN BUS INJECTION.

PROJECT OBJECTIVE

- BYPASS ABS AND LIMP MODE VIA CAN BUS INJECTION ATTACK
- ENABLE A VEHICLE'S OPERATION DESPITE ERROR STATES AND BATTLE DAMAGE
- CREATE USER-FRIENDLY DEVICE FOR EASY MILITARY FIELD ACCESSIBILITY
- DESIGN A SMALL LOW-COST PROTOTYPE

TECHNICAL PROCESS

- ACCESS THE CAN BUS THROUGH THE HEADLIGHT WIRING
- IMPLEMENT AUTHENTICATION ATTACK FOR DOOR LOCKS AND STARTER MOTOR
- USE CANALYZER FOR TRAFFIC MONITORING AND REVERSE ENGINEERING ECU BEHAVIOR
- ACTIVELY SUPPRESS ERROR MESSAGES THAT MIGHT DISABLE THE VEHICLE

ETHICS - SAFETY - SUSTAINABILITY

- ETHICS: INCREASES OPERATOR SAFETY DURING CRITICAL OPERATIONS
- SAFETY: PREVENTS MALFUNCTION DURING COMBAT BY BYPASSING RESTRICTIVE SAFETY FEATURES
- SUSTAINABILITY: REPURPOSES EXISTING CIVILIAN VEHICLES FOR MILITARY USE

FIGURE 1: DECODING DIFFERENTIAL CAN FRAMES

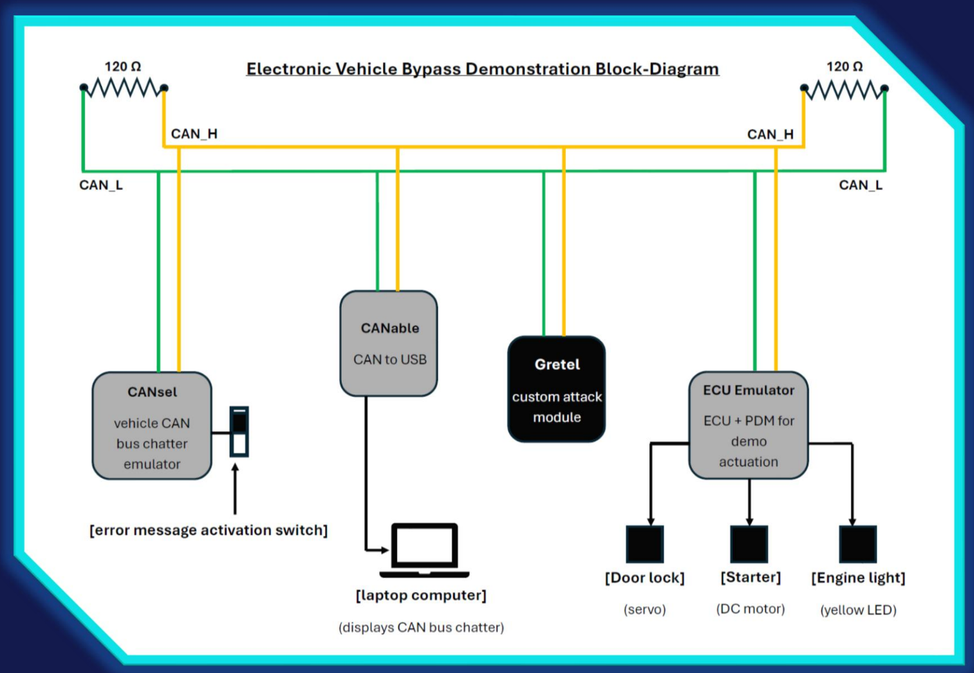

FIGURE 2: SYSTEM BLOCK DIAGRAM

SYSTEM DESIGN

-- PROTOTYPE OVERVIEW - GRETEL V1 & V2 --

- GRETEL V1: BUILT USING ARDUINO R3 WITH CAN SHIELD AND CUSTOM CONTROL BOARD
- MODE SELECTOR:
  - * INJECTION MODE: SENDS UNLOCK/START FRAMES
  - * SUPPRESSION MODE: LAUNCHES REDOS ATTACK TO SUPPRESS ERROR FRAMES

SIMULATION ENVIRONMENT VIA THE DEMO BOARD: TRANSMITTING ECU EMULATOR (CANSEL), RECEIVING ECU/PDM NODE WITH ACTUATORS, CANABLE AND CAN BUS WIRING WITH 120Ω TERMINATION RESISTORS

-- GRETEL V2 UPGRADES --

- CREATE A MORE COMPACT MODEL
- INCORPORATE A NANO MICROCONTROLLER WITH A CAN SHIELD & BUILT-IN OBD2 INTERFACE
- MAINTAIN FULL FUNCTIONALITY

IMPLEMENTATION

- CAN BUS LOOP: PROVIDES A NETWORK FOR NODAL COMMUNICATION
- CANSEL NODE: INJECTS ARBITRARY CAN CHATTER FRAMES AND ERROR FRAMES
- CANABLE USB MONITOR: ANALYZING BUS TRAFFIC
- ECU / PDM NODE: RECEIVER NODE, EMULATES REAL WORLD RESPONSE (SERVO, MOTOR, LED)
- ATTACK NODE: PERFORMS CAN BUS INFILTRATION

BUDGET SUMMARY

COMPONENT	UNIT PRICE	QUANTITY	ITEM TOTAL
ARDUINO UNO R3 - CLONE	7.19	3	21.57
SEEED STUDIO CAN BUS SHIELD	27.19	3	81.57
CAN TO USB3 CONVERTER	16.08	1	16.08
MKR CAN SHIELD	38.99	1	38.99
ARDUINO NANO	24.90	1	24.90
		TOTAL:	183.11

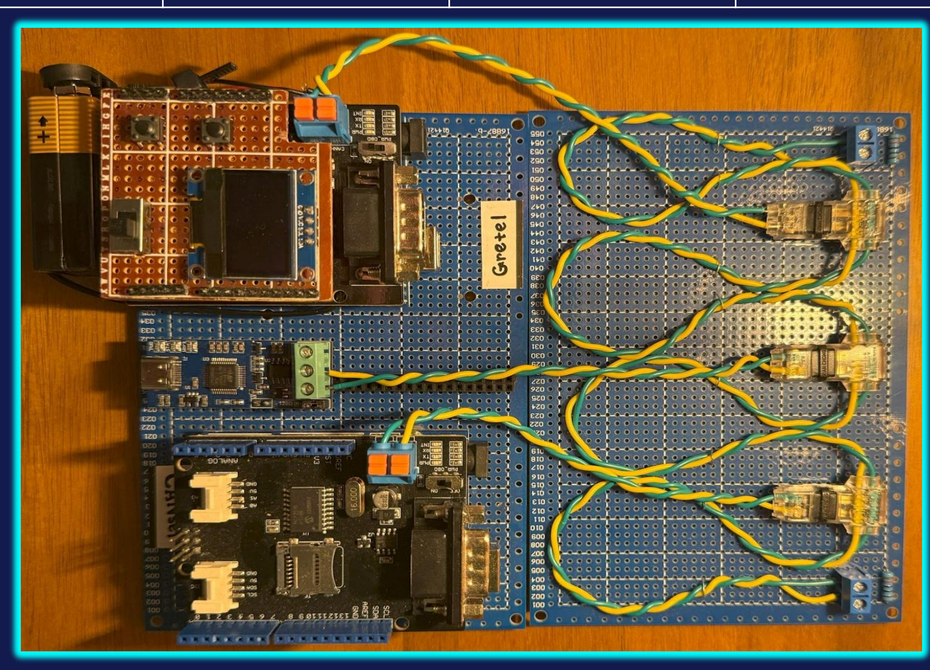

FIGURE 3: CANSEL - CANABLE - CAN BUS LOOP - GRETEL V1

CONCLUSION

THIS PROJECT ADDRESSES THE NEED TO BYPASS CRITICAL SAFETY AND ANTI-THEFT FEATURES IN NON-MILITARY VEHICLES THAT MAY BE USED IN COMBAT SCENARIOS. THESE FEATURES CAN PREVENT OPERATION IN CRITICAL SITUATIONS, SO OPERATORS MUST HAVE TOOLS TO ADAPT VEHICLE FUNCTIONALITY AS NEEDED.
BY SIMULATING A VEHICLE'S CAN BUS, WE HAVE DEVELOPED A PROTOTYPE CAPABLE OF LISTENING AND INJECTING MESSAGES. WHEN ERROR MESSAGES ARE DETECTED, IT FLOODS THE BUS WITH HIGH-PRIORITY FRAMES TO PLACE THE VEHICLE IN ERROR-PASSIVE MODE. COMPUTER SOFTWARE WAS USED TO MONITOR CAN BUS TRAFFIC AND VERIFY THE PROTOTYPE'S EFFECTIVENESS.