O SCALE MODEL RAILROADING
ELECTRICAL, COMPUTER & SIGNAL ENGINEERING CAPSTONE

Senior Year | Full-Semester Design Project | Professional Consulting Report

Power Electronics · Digital Signal Processing · Embedded Systems
Control Theory · Communications & Networking · FPGA & Real-Time Systems
RF & Electromagnetic Compatibility · Cybersecurity & Safety-Critical Systems

Client: Pocono Valley Short Line Railroad

Course Title	Precision Railroad Electronics: A Senior Capstone in Electrical, Computer & Signal Engineering
Target Students	Senior EE / CE / Signal Engineering — Year 4, Full Semester (15 weeks)
Prerequisites	Digital Signal Processing; Control Systems; Embedded Systems; Communications Theory; Power Electronics; Probability & Stochastic Processes; Computer Architecture
Client	Pocono Valley Short Line Railroad (simulated industry client with real technical specifications)
Deliverable	Professional Engineering Consulting Report — equivalent to a real-world System Design Report submitted to a railroad client
Module 1	Power Systems Engineering — DCC Traction Power, EMI/EMC & Arc Flash Analysis (Weeks 1–3)
Module 2	Digital Signal Processing & Control — Adaptive Speed Control, PID Tuning & Kalman Filtering (Weeks 4–6)
Module 3	Embedded Systems & Real-Time Computing — FPGA-Based Interlocking, RTOS & Safety-Critical Software (Weeks 7–9)
Module 4	Communications & Network Engineering — Wireless Control, CAN Bus, Cybersecurity & Protocol Design (Weeks 10–12)
Module 5	Systems Integration & Verification — HIL Testing, Fault Injection & System-Level Validation (Weeks 13–14)
Capstone Week	Final Consulting Report Delivery & Client Presentation (Week 15)
ABET Coverage	Student Outcomes (1)(2)(3)(4)(5)(6)(7) — comprehensive senior-level ABET evidence

IEEE Standards	IEEE 1482.1 (DCC), IEEE 693 (seismic), IEEE 519 (harmonics), IEC 62280 (railway cybersecurity), NFPA 70E (arc flash)
Contact	O Scale STEM Education Initiative

Capstone Design Philosophy: This capstone treats the O Scale model railroad as a fully instrumented 1:48 scale electrical and signal engineering laboratory. Every module produces a section of the final Professional Consulting Report — the same document format used by engineering firms retained by Class I railroads. By Week 15, teams deliver a complete System Design Report covering power architecture, control algorithms, embedded software specification, communications security, and system-level test validation. The report is reviewed against real IEEE and IEC standards. The client expects professional-grade work.

Client Brief — Pocono Valley Short Line Railroad

Client Statement: The Pocono Valley Short Line Railroad (PVSLR) operates 12 miles of track between Stroudsburg and Tobyhanna, Pennsylvania. The railroad is upgrading its entire traction control, signaling, and communications infrastructure from legacy analog systems to a modern digital architecture. PVSLR has retained your engineering firm to deliver a complete System Design Report covering: (1) DCC traction power system redesign with EMI/EMC compliance; (2) adaptive locomotive speed control with real-time state estimation; (3) FPGA-based signal interlocking and safety-critical embedded software; (4) wireless and wired communications network with cybersecurity provisions; and (5) system integration test plan with formal verification evidence. The railroad operates under FRA oversight and must comply with all applicable IEEE and IEC standards. The final report will be submitted to the PVSLR Board of Directors and will form the basis for a capital investment decision.

ABET Student Outcomes Coverage

Standard/Code	Core Competency	How the Lab Module Addresses It
ABET (1)	Identify, formulate, solve complex EE/CE problems using math, science, engineering	Every module requires derivation-based solutions, experimental measurement, and comparison to published standards
ABET (2)	Apply engineering design satisfying specified needs with realistic constraints	Each module section becomes part of the client deliverable — a real design document with real constraints (cost, regulatory, safety)
ABET (3)	Communicate effectively in written and oral forms to technical and non-technical audiences	Weekly written progress reports; formal consulting report; client presentation to non-engineer "board members"
ABET (4)	Recognize ethical and professional responsibilities; make informed judgments	Module 3 (safety-critical software), Module 4 (cybersecurity), and the capstone ethics statement address ABET (4) explicitly
ABET (5)	Function effectively in a team with diverse roles and responsibilities	Roles rotate each module: Systems Engineer, Lead Analyst, Technical Writer, Test Engineer, Client Liaison

ABET (6)	Develop and conduct experiments; analyze and interpret data	Each module includes a laboratory investigation on the O Scale layout with data collection, analysis, and error quantification
ABET (7)	Acquire and apply new knowledge from published standards and research literature	Each module introduces one IEEE/IEC standard students must read, interpret, and apply to their design

Full-Semester Schedule

Week	Phase	Activities & Deliverables	EE/CE/Signal Thread
1	Kickoff	Client brief review; team formation; role assignment; system requirements analysis; O Scale layout electrical survey	Requirements Engineering
2	M1 Lab	DCC power system measurement: voltage, current, THD, frequency spectrum analysis	Power Electronics / EMC
3	M1 Report	Module 1 consulting report section drafted; EMI/EMC compliance gap analysis completed	Power Quality / NFPA 70E
4	M2 Lab	Speed control experiment: open-loop step response; closed-loop PID tuning; back-EMF measurement	Control Systems
5	M2 Lab	Kalman filter implementation: state estimation of loco position and velocity from noisy sensors	DSP / Estimation Theory
6	M2 Report	Module 2 consulting report section; Bode plot analysis; stability margins documented	Control Theory
7	M3 Lab	FPGA interlocking logic design; state machine implementation; timing analysis	Digital Systems / FPGA
8	M3 Lab	RTOS task scheduling; worst-case execution time (WCET) analysis; safety integrity level (SIL) evaluation	Embedded / Safety-Critical
9	M3 Report	Module 3 consulting report section; DO-178C software quality checklist; SIL justification	Software Safety
10	M4 Lab	CAN bus protocol implementation; message timing analysis; wireless link budget calculation	Communications Engineering
11	M4 Lab	Cybersecurity threat modeling (STRIDE); penetration test on simulated DCC network; IEC 62280 gap analysis	Cybersecurity / Networking
12	M4 Report	Module 4 consulting report section; security architecture diagram; residual risk register	Network Security
13	M5 Lab	Hardware-in-the-loop (HIL) test setup; fault injection testing; system-level performance measurement	Systems Integration
14	M5 Report	Verification & validation report section; test coverage matrix; non-conformance register	V&V / Quality
15	Capstone	Final consulting report delivery; 30-minute client	Professional Practice

		presentation; individual reflection	

Materials — Full Semester

Item	Qty/Team	Specification
O Scale DCC layout (minimum 4×8 ft, with 3 independent block sections, 2 sidings, 1 passing loop)	1	Pre-wired with feeder bus; must have accessible terminal strips for measurement attachment
DCC Command Station + 2 Boosters (e.g., Digitrax DCS210+)	1 set	DCC compliant; minimum 5A per booster; supports programming track
DCC-equipped locomotives (minimum 3, different decoder manufacturers)	3	Include one sound decoder, one back-EMF decoder, one basic decoder for comparison
Digital oscilloscope (4-channel, 100 MHz minimum bandwidth)	1 per team	Rigol DS1054Z or equivalent; must capture DCC waveform and FFT
True-RMS power analyzer (e.g., Fluke 435-II or equivalent)	1	For THD, power factor, harmonic spectrum measurement
FPGA development board (Xilinx Artix-7 or Intel Cyclone V)	1 per team	Vivado or Quartus free student license; minimum 100 I/O pins
Raspberry Pi 4 or equivalent SBC (for RTOS experiments)	1 per team	FreeRTOS or Zephyr RTOS; Python + C development environment
CAN bus transceiver modules (MCP2515 + TJA1050)	2 per team	SPI-to-CAN; connect to SBC for bus protocol experiments
2.4 GHz wireless module (ESP32 or nRF52840)	2 per team	For link budget and interference experiments
Current probe (clamp-on, AC/DC, 1 mA resolution)	1 per team	For non-invasive current measurement on DCC bus
Spectrum analyzer (or SDR: RTL-SDR dongle + laptop)	1	For EMI radiated emissions characterization
Precision resistor decade box (0.1Ω resolution, 10W)	1	For load simulation and fault injection
Logic analyzer (Saleae Logic 8 or equivalent)	1 per team	For CAN bus, SPI, UART protocol decode
Engineering logbooks (bound, quad-ruled)	1 per student	Professional documentation; kept throughout semester
Laptop with MATLAB/Simulink (student license) or GNU Octave + Python	1 per student	DSP, control system simulation, Kalman filter implementation

MODULE 1

Power Systems Engineering

DCC Traction Power Architecture, Power Quality, EMI/EMC Compliance & Arc Flash Analysis

Duration	3 weeks (Weeks 1–3): 1 week theory + 2 weeks lab + report section
EE/CE Threads	Power Electronics · Power Quality · Electromagnetic Compatibility (EMC) · Electrical Safety
ABET Outcomes	(1) Formulate and solve power engineering problems; (6) Design and conduct experiments; (7) Apply IEEE 519 and NFPA 70E
Core Concepts	DCC AC waveform analysis, harmonic distortion (THD), power factor correction, conducted and radiated EMI, electromagnetic compatibility (EMC), arc flash incident energy, Fourier series, impedance matching, transmission line effects on long layouts
Math Required	Fourier series and FFT, complex impedance, phasor analysis, power factor calculations, decibel (dB) scale, skin effect at high frequency, transmission line equations
IEEE Standards	IEEE 519-2022 (Harmonic Control in Electric Power Systems); NFPA 70E-2021 (Electrical Safety in the Workplace); FCC Part 15 (unintentional radiators)
Consulting Report Section	Section 2: Traction Power System Design — Power Architecture, Power Quality Analysis, EMI/EMC Compliance Assessment

Industry Context

DCC power systems are not simple DC supplies — they deliver a modified square-wave AC signal at 14.5–22V RMS at frequencies between 4–8 kHz, superimposed with digital data packets. This waveform is rich in odd harmonics, generates significant conducted and radiated EMI, and can cause interference with sensitive signal equipment on the same layout. In full-scale railroad applications, traction power systems are regulated by IEEE 519 for harmonic distortion limits, and all electrical work must comply with NFPA 70E for worker safety. The IEEE 1482.1 standard governs DCC interoperability. Senior engineers are expected to design to these standards — not merely acknowledge them.

Theoretical Foundations

1.1 — DCC Waveform Fourier Analysis

The DCC track signal is a bipolar square wave with asymmetric half-cycles encoding binary data. A periodic square wave of amplitude A and period T has the Fourier series:

```
v(t) = (4A/pi) * [sin(w0*t) + (1/3)sin(3*w0*t) + (1/5)sin(5*w0*t) + ...]
```

Where w0 = 2*pi/T is the fundamental angular frequency. The nth harmonic has amplitude 4A/(n*pi). For a DCC signal at 8 kHz fundamental, significant harmonics exist at 24 kHz, 40 kHz, 56 kHz — all within the AM broadcast band and potentially interfering with onboard sound decoder audio circuits.

1.2 — Total Harmonic Distortion (THD)

```
THD = sqrt(V2^2 + V3^2 + V4^2 + ...) / V1 * 100%
```

IEEE 519 limits THD at the point of common coupling (PCC). For DCC systems, the "PCC" is the track bus. Students measure THD using the oscilloscope FFT function and the power analyzer. IEEE 519-2022 Table 2 limits individual harmonic voltages to 3% of fundamental for systems below 1 kV. DCC harmonic content routinely exceeds this — students analyze the compliance gap and propose mitigation (LC filter, ferrite choke placement, booster isolation).

1.3 — Transmission Line Effects on Long Layouts

A DCC bus longer than approximately 3 meters begins to exhibit transmission line behavior. The characteristic impedance:

```
Z0 = sqrt((R + jwL)/(G + jwC))
```

For typical 14 AWG layout bus wire: L ≈ 0.25 µH/m, C ≈ 100 pF/m, giving Z0 ≈ 50Ω at high frequency. Reflections occur when the load impedance does not match Z0. The reflection coefficient:

```
Gamma = (ZL - Z0)/(ZL + Z0)
```

Students measure voltage standing wave ratio (VSWR) on a long layout bus and calculate the impedance mismatch. They then propose a termination resistor value to minimize reflections and verify the improvement on the oscilloscope.

1.4 — EMI: Conducted vs. Radiated Emissions

Conducted emissions travel along wires; radiated emissions propagate through space. FCC Part 15B limits radiated emissions from unintentional radiators (which includes DCC boosters and their wiring). Students use an RTL-SDR dongle as a spectrum analyzer to characterize the radiated emissions from the DCC layout bus and compare to FCC Part 15B Class B limits (which apply to residential use — the most restrictive).

1.5 — Arc Flash Incident Energy Analysis

NFPA 70E requires arc flash hazard analysis for any electrical system where workers may be exposed during energized work. Even though DCC voltages are low, the analysis methodology is a professional competency. Incident energy E at working distance D from an arc fault:

```
E = 4.184 * Cf * En * (t/0.2) * (610^x / D^x)   [cal/cm^2]
```

Where Cf = calculation factor; En = normalized incident energy; t = arcing time (s); D = working distance (mm); x = distance exponent. Students calculate the arc flash PPE category for the DCC booster panel using NFPA 70E Table 130.7(C)(15)(a) and specify required PPE.

Laboratory Investigation — Module 1

Experiment 1A — DCC Waveform Characterization (90 min)

Using the 4-channel oscilloscope connected to the DCC track bus:

1. Capture the DCC waveform with no locomotive load. Record: peak-to-peak voltage, RMS voltage (true RMS function), fundamental frequency, and duty cycle of "1" bits vs. "0" bits.
2. Enable the FFT function. Capture the harmonic spectrum. Record amplitude (dBV) at fundamental, 3rd, 5th, 7th, 9th, and 11th harmonics. Calculate THD from the measured harmonic amplitudes.
3. Connect a load resistor simulating two locomotives (total ≈ 1Ω). Repeat waveform and FFT capture. Compare THD with and without load. Explain the difference.
4. Place an LC low-pass filter (L = 100µH, C = 470nF) in series with one rail. Repeat FFT capture. Quantify harmonic attenuation at each frequency. Did the filter affect the DCC data signal? How do you know?
5. Calculate the filter cutoff frequency: fc = 1/(2*pi*sqrt(LC)). Compare to DCC fundamental frequency. Is the filter correctly placed in the frequency spectrum?

Experiment 1B — Transmission Line Measurement (60 min)

Connect a 20-foot length of 14 AWG bus wire as a DCC feeder. Measure rail-to-rail voltage at 0, 5, 10, 15, and 20 feet. Calculate the impedance per foot from the voltage drop. Estimate the characteristic impedance Z0 from the wire geometry. Observe reflections on the oscilloscope with an open-circuit far end vs. a matched termination resistor. Calculate the VSWR for each case.

Experiment 1C — Radiated EMI Spectrum Survey (60 min)

Using the RTL-SDR dongle and SDR# or GNU Radio software, sweep the spectrum from 1 MHz to 200 MHz with the antenna placed 1 meter from the DCC layout bus. Record peak emissions at each DCC harmonic frequency. Compare to FCC Part 15B Class B limits (provided as a reference table). Identify the frequency of maximum emission. Wrap 10 turns of the bus wire through a Fair-Rite 31-material toroid ferrite and repeat the sweep. Quantify attenuation in dB at each peak frequency.

Experiment 1D — Power Budget & Efficiency Analysis (45 min)

Using the true-RMS power analyzer at the booster input: measure real power (W), apparent power (VA), reactive power (VAR), and power factor (PF) under three load conditions: no load, two locomotives running, full rated load (4 locomotives + accessories). Calculate system efficiency at each load point: eta = P_output / P_input * 100%. Plot efficiency vs. load percentage. Identify the optimal operating point. Calculate annual energy cost at $0.13/kWh for a 4-hour daily operation schedule.

Module 1 Consulting Report Section Requirements

Section 2 of the final consulting report must include:

- Executive Summary: one paragraph — key findings and recommendations for a non-engineer reader
- Power Architecture Diagram: one-line diagram of the complete DCC power system with booster ratings, feeder lengths, circuit breaker locations, and district boundaries
- Power Quality Analysis: THD measured values vs. IEEE 519 limits; harmonic spectrum plots; filter design specification with fc, component values, and insertion loss

- Transmission Line Analysis: characteristic impedance calculation; VSWR measurements; termination recommendation with supporting equations
- EMI/EMC Compliance Assessment: radiated emissions spectrum vs. FCC Part 15B limits; compliance gap table; mitigation measures with quantified dB improvement
- Arc Flash Hazard Analysis: incident energy calculation; PPE category determination per NFPA 70E; required approach distances; recommended safe work practices
- Power Budget: efficiency curve; annual energy cost; recommendation for power factor correction if PF < 0.85

Standards & ABET Alignment — Module 1

Standard/Code	Core Competency	How the Lab Module Addresses It
IEEE 519-2022	Harmonic distortion limits for power systems	Students measure THD and compare to Table 2 limits; design LC filter to achieve compliance
FCC Part 15B	Radiated emission limits for unintentional radiators	Students measure layout emissions vs. FCC limits; design ferrite mitigation; quantify compliance improvement
NFPA 70E-2021	Arc flash PPE requirements	Students perform arc flash calculation using NFPA 70E methodology; specify PPE category for DCC panel work
IEEE 1482.1	DCC standard — packet timing, voltage levels, signal integrity	Students verify DCC waveform compliance with timing specs from the standard
ABET (1)	Formulate and solve complex EE problems	Fourier analysis, transmission line analysis, and filter design are all formally derived engineering problems
ABET (6)	Design and conduct experiments; analyze data	All four experiments include theoretical prediction, experimental measurement, and percent-error analysis

Assessment — Module 1

Criterion	4 – Exemplary	3 – Proficient	2 – Developing	1 – Beginning
Fourier / THD Analysis	Fourier series of DCC waveform derived; THD calculated from FFT measurements; IEEE 519 compliance gap quantified; filter designed with correct fc; insertion loss measured and compared to	THD calculated; IEEE 519 compared; filter designed; insertion loss measured	THD calculated; IEEE 519 compared; filter designed without insertion loss verification	THD calculated; no IEEE 519 comparison; no filter design

	prediction			
Transmission Line Analysis	Z0 calculated from wire geometry; VSWR measured for open and matched cases; termination value calculated and verified; reflection waveform identified on oscilloscope	Z0 calculated; VSWR for both cases measured; termination value calculated	Z0 calculated; VSWR for one case; termination value calculated without verification	Transmission line concept explained without measurement or calculation
EMI Spectrum Survey	Spectrum captured at 1m; peaks at DCC harmonics identified and recorded in dBV; compared to FCC Part 15B limits in table format; ferrite attenuation quantified in dB at each peak	Spectrum captured; peaks identified; FCC compared; ferrite attenuation at primary peak	Spectrum captured; peaks identified; FCC not compared numerically	Spectrum captured; no harmonic identification; no FCC comparison
Power Budget	P, Q, S, PF measured at 3 load points; efficiency calculated and plotted; optimal operating point identified; annual energy cost calculated; PF correction recommendation stated	All quantities measured; efficiency plotted; energy cost calculated; PF recommendation	P and PF measured; efficiency at one load point; energy cost calculated	Power measured at one load; no efficiency plot; no energy cost
Consulting Report Section	Professional format: executive summary, one-line diagram, all required sections present, IEEE/FCC references cited by standard number and clause, all figures captioned, units	All sections present; most references cited; minor formatting gaps	Most sections present; references cited generically; figure captions missing	Report section is informal lab write-up; missing multiple required sections

	consistent throughout			

MODULE 2

Digital Signal Processing & Control Systems

Adaptive Speed Control, Back-EMF Estimation, PID Tuning & Kalman Filtering

Duration	3 weeks (Weeks 4–6)
EE/CE Threads	Control Systems · Digital Signal Processing · Estimation Theory · State-Space Methods
ABET Outcomes	(1)(2)(6)(7) — formulate control problem, design experiment, apply Kalman filter from literature
Core Concepts	Transfer function, open-loop vs. closed-loop control, PID control, Bode plot, gain/phase margin, Nyquist criterion, state-space representation, Kalman filter (KF), back-EMF speed estimation, Z-transform, digital PID implementation
Math Required	Laplace transform, Z-transform, complex frequency response H(jw), matrix algebra (Riccati equation for KF), differential equations (state-space), least-squares curve fitting
IEEE Standards	IEEE 1076 (VHDL — for future FPGA implementation); IEEE 754 (floating point — for numerical precision in digital PID)
Consulting Report Section	Section 3: Adaptive Locomotive Speed Control System Design — Transfer Function, PID Tuning, State Estimation & Performance Specification

Industry Context

Modern DCC decoders implement back-EMF (BEMF) speed control — the locomotive motor's back-EMF voltage, which is proportional to shaft speed, is sampled during brief power interruptions and used as the feedback signal in a closed-loop speed controller. This is equivalent to an industrial motor speed controller. The engineering challenge: the motor-drivetrain system has nonlinear dynamics that vary with load, grade, and track conditions. Advanced decoders use adaptive control algorithms. Senior engineers designing the next generation of DCC decoder firmware must understand the complete control system — from plant dynamics to digital filter implementation to stability analysis.

Theoretical Foundations

2.1 — DC Motor Transfer Function

The DC motor driving an O Scale locomotive can be modeled as a second-order system. Applying KVL and Newton's second law:

```
V_a(s) = (La*s + Ra)*I_a(s) + Kb*Omega(s)
Kt*I_a(s) = (J*s + b)*Omega(s)
```

Eliminating I_a(s), the transfer function from armature voltage V_a to angular velocity Omega:

```
G(s) = Omega(s)/V_a(s) = Kt / [(La*s+Ra)(J*s+b) + Kt*Kb]
```

For small motors (La << Ra/b), the electrical time constant is negligible and G(s) simplifies to:

```
G(s) ≈ Km / (tau_m*s + 1)   where Km = 1/Kb, tau_m = Ra*J/(Kb*Kt + Ra*b)
```

Students measure Km and tau_m experimentally from a step response and compare to the theoretical values derived from motor nameplate data.

2.2 — PID Controller Design & Tuning

```
C(s) = Kp + Ki/s + Kd*s   [continuous PID]
```

Tuning criteria: Phase Margin (PM) >= 45 degrees for adequate stability; Gain Margin (GM) >= 6 dB. Students use Bode plot analysis to determine the crossover frequency and adjust Kp, Ki, Kd to meet the PM and GM specifications. The digital implementation uses the Tustin (bilinear) transformation:

```
s = 2/T * (z-1)/(z+1)   [Tustin discretization]
C(z) = [Kp + Ki*T/2*(z+1)/(z-1) + Kd*2/T*(z-1)/(z+1)]
```

2.3 — Back-EMF Speed Estimation

During a brief PWM off-period (approximately 100 µs for DCC decoders), the motor back-EMF can be measured directly:

```
BEMF = V_measured_during_off_period ≈ Kb * omega
omega_estimated = BEMF / Kb
```

This is a noisy measurement — rail resistance, contact resistance, and switching transients corrupt the signal. Students implement a first-order IIR low-pass filter to reduce noise:

```
y[n] = alpha*x[n] + (1-alpha)*y[n-1]   where alpha = 1 - e^(-T/tau)
```

2.4 — Kalman Filter for Position & Velocity Estimation

The Kalman filter provides the optimal linear state estimator for a system with Gaussian process and measurement noise. State vector x = [position; velocity]. State space model:

```
x[k+1] = F*x[k] + G*u[k] + w[k]   [process model; w ~ N(0,Q)]
z[k] = H*x[k] + v[k]              [measurement model; v ~ N(0,R)]
```

For constant-velocity model between track sensors: F = [1 T; 0 1], G = [T^2/2; T], H = [1 0]. The Kalman filter two-step cycle:

```
Predict:  x_hat[-] = F*x_hat[+],   P[-] = F*P[+]*F' + Q
Update:   K = P[-]*H'*(H*P[-]*H' + R)^(-1)
          x_hat[+] = x_hat[-] + K*(z - H*x_hat[-])
          P[+] = (I - K*H)*P[-]
```

Students implement the Kalman filter in Python/MATLAB, tune Q and R matrices using measured sensor noise statistics, and compare estimated position/velocity to ground truth measured by a reference encoder.

Laboratory Investigation — Module 2

Experiment 2A — Motor System Identification (60 min)

Apply a step voltage to the locomotive motor (isolated from DCC, using a bench DC supply) and capture the shaft speed response using a tachometer or optical encoder. Fit an exponential curve to

extract Km and tau_m. Verify by applying a ramp input and comparing measured vs. predicted output. Measure back-EMF constant Kb by spinning the motor externally and measuring open-circuit terminal voltage vs. speed.

Experiment 2B — PID Controller Tuning (75 min)

Implement a digital PID controller on the Raspberry Pi / SBC. Connect BEMF measurement to the ADC input. Output PWM duty cycle to a motor driver. Starting with Ziegler-Nichols initial estimates: increase Kp until sustained oscillation (ultimate gain Ku); note ultimate period Tu; calculate PID parameters: Kp = 0.6*Ku, Ki = 1.2*Ku/Tu, Kd = 0.075*Ku*Tu. Plot step response. Measure: rise time, settling time, overshoot, steady-state error. Adjust Ki to eliminate steady-state error on a 2% grade (apply grade by tilting track section). Plot Bode plot of open-loop transfer function L(jw) = C(jw)*G(jw) using frequency sweep. Measure phase margin and gain margin. Do they meet the >= 45 deg / >= 6 dB specifications?

Experiment 2C — Kalman Filter Implementation & Validation (90 min)

Install two infrared beam-break sensors at known positions on the layout. Sensor z[k] = position (binary: car present or not). Between sensors, velocity is estimated by the filter. Initialize Q = diag([0.01, 0.1]) and R = 0.5 (measurement noise variance measured from sensor jitter). Run the locomotive at 3 speed settings. For each: record sensor timestamps; run the Kalman filter in post-processing; plot estimated position and velocity vs. time. Compare estimated velocity to tachometer ground truth. Calculate RMS estimation error. Tune Q and R to minimize RMS error. Explain the trade-off between Q (process trust) and R (measurement trust) in the context of railroad train tracking.

Experiment 2D — Grade Rejection & Disturbance Response (45 min)

Operate the PID-controlled locomotive up a 3% grade (simulate by tilting a track section). Record: speed before grade, speed sag entering grade, recovery time, final steady-state speed on grade. Measure integral windup if Ki is too large. Implement anti-windup (clamp the integrator output) and compare the step response with and without anti-windup. Calculate the load disturbance rejection ratio: DR = delta_speed_without_control / delta_speed_with_control.

Module 2 Consulting Report Section Requirements

- Motor Transfer Function: G(s) derived analytically and from system identification; Km and tau_m comparison table; percent error and explanation
- PID Controller Design: design specifications (PM, GM, rise time, overshoot); Bode plots of L(jw) before and after tuning; Z-domain implementation with Tustin coefficients; step response plots annotated with performance metrics
- BEMF Speed Estimator: measurement circuit description; IIR filter design with cutoff frequency and alpha calculation; noise analysis (measured SNR before and after filtering)
- Kalman Filter: state space model matrices F, G, H stated with physical justification; Q and R matrices with tuning rationale; estimated vs. ground truth plots; RMS error table; discussion of filter limitations
- Grade Rejection Performance: disturbance rejection ratio; anti-windup implementation; specification for maximum allowable speed deviation on 3% grade (student must set this specification based on railroad operations context)

Assessment — Module 2

Criterion	4 – Exemplary	3 – Proficient	2 – Developing	1 – Beginning
System Identification	Km and tau_m extracted from step response with curve fit shown; Kb measured independently; transfer function G(s) written with numerical values; percent error vs. nameplate calculated	Km and tau_m from step response; G(s) written; Kb measured; no percent error	Km and tau_m from step response; G(s) written; Kb not independently measured	Step response captured; G(s) stated without parameter identification
PID Design & Stability	Bode plot of L(jw) plotted from frequency sweep; PM and GM measured and compared to specification; step response annotated with all performance metrics; Ziegler-Nichols rationale documented	Bode plot plotted; PM and GM measured; step response annotated; Z-N rationale stated	Bode plot from simulation only; PM and GM measured; step response annotated	PID parameters chosen; no Bode plot; no stability margin analysis
Kalman Filter Implementation	KF implemented in code; Q and R tuned from measured noise statistics; estimated vs. ground truth plotted for 3 speed settings; RMS error calculated; Q-R trade-off explained	KF implemented; Q and R tuned; estimated vs. truth plotted; RMS error calculated	KF implemented with default Q and R; estimated vs. truth plotted; RMS error calculated	KF equations stated; not implemented; no experimental data

Grade Disturbance Rejection	Disturbance rejection ratio calculated with and without control; anti-windup implemented and compared; speed specification set with engineering justification; integral windup phenomenon explained	DR calculated; anti-windup compared; speed specification stated	DR calculated; anti-windup not implemented; specification stated without justification	Speed sag measured; no DR calculation; no anti-windup
Digital Implementation	Tustin discretization shown step-by-step; z-domain transfer function C(z) stated; sampling rate justified relative to system bandwidth (Nyquist); fixed-point overflow risk assessed	Tustin shown; C(z) stated; sampling rate justified	Tustin shown; C(z) stated; sampling rate stated without justification	Digital PID implemented without Tustin derivation or sampling analysis

MODULE 3

Embedded Systems & Safety-Critical Software

FPGA Interlocking Logic, RTOS Task Scheduling, WCET Analysis & SIL Determination

Duration	3 weeks (Weeks 7–9)
EE/CE Threads	Digital Systems / FPGA · Embedded Systems · Real-Time Operating Systems · Safety-Critical Software Engineering
ABET Outcomes	(1)(2)(4)(6)(7) — ABET (4) explicitly addressed through SIL and DO-178C ethics
Core Concepts	Finite state machine (FSM) design, FPGA implementation (VHDL/Verilog), RTOS task model, rate monotonic scheduling (RMS), worst-case execution time (WCET), Safety Integrity Level (SIL), DO-178C software quality levels, formal verification (model checking), fault tree analysis for software
Math Required	Boolean algebra, FSM state transition matrices, RMS schedulability test (sum of utilizations), WCET analysis, reliability block diagrams, fault tree probability
Standards Applied	IEC 61508 (Functional Safety of Electrical/Electronic/Programmable Safety-Related Systems); IEC 62425 (Railway safety-related electronic systems); DO-178C (Software Considerations in Airborne Systems) — analogous to railway practice
Consulting Report Section	Section 4: Signal Interlocking System Design — FPGA Architecture, RTOS Specification, Software Safety Case & SIL Justification

Industry Context

Railroad signal interlocking systems are among the most safety-critical electronic systems in civil infrastructure. A failure of the interlocking — the system that prevents conflicting train movements — can result in head-on collisions. The FRA mandates Positive Train Control (PTC) on all Class I railroads, and PTC software must meet stringent safety requirements derived from IEC 62425 and IEC 61508. The Safety Integrity Level (SIL) framework quantifies the required probability of dangerous failure per hour: SIL 4 requires PFH < 10^-8 per hour — more reliable than virtually any other engineered system. Students design a simplified interlocking in FPGA and evaluate its SIL.

Theoretical Foundations

3.1 — Finite State Machine Design for Interlocking

A railroad interlocking grants routes (combinations of switch positions and signal aspects) to trains while preventing conflicting routes from being set simultaneously. The interlocking logic is a combinational and sequential digital system. For a simple junction with 2 routes (Route A: straight through; Route B: diverging to siding), the interlocking truth table:

Train A Req.	Train B Req.	Switch Pos.	Signal A	Signal B / Interlock Logic

0	0	Either	Stop	Stop — no requests
1	0	Normal	Clear	Stop — A has priority
0	1	Reverse	Stop	Clear — B has diverging route
1	1	Normal	Clear	Stop — conflict! Only one can proceed

Students extend this to a 4-route interlocking, design the complete FSM (states: IDLE, ROUTE_A_LOCKED, ROUTE_B_LOCKED, CONFLICT_LOCKOUT), implement in VHDL, synthesize on the FPGA, and verify using testbench simulation.

3.2 — Rate Monotonic Scheduling (RMS)

For an RTOS with n periodic tasks, Rate Monotonic Scheduling assigns priority by period (shorter period = higher priority). The schedulability test (Liu & Layland 1973):

```
sum(Ci/Ti) <= n*(2^(1/n) - 1)
```

Where Ci = worst-case execution time (WCET) of task i; Ti = period of task i. As n -> infinity, the bound approaches ln(2) ≈ 0.693. If the utilization sum exceeds this bound, RMS cannot guarantee all deadlines will be met. Students define tasks for the DCC interlocking system and verify RMS schedulability.

Task	Period Ti (ms)	WCET Ci (ms)	Utilization Ci/Ti	Priority (RMS)
Track occupancy sensor polling	10	0.8		1 (highest)
Interlocking logic evaluation	20	2.5		2
Signal aspect update (output)	50	1.2		3
DCC packet generation	8	1.5		4
Speed controller PID loop	100	5.0		5
Telemetry / logging	500	15.0		6 (lowest)
TOTALS	—	—		

3.3 — Safety Integrity Level (SIL) Determination

IEC 61508 defines four Safety Integrity Levels. The target SIL is determined by the risk reduction required from the safety function. For a railroad interlocking:

```
PFH_required = (Acceptable_risk) / (Frequency_of_hazardous_event)
```

SIL 1: 10^-5 <= PFH < 10^-4; SIL 2: 10^-6 <= PFH < 10^-5; SIL 3: 10^-7 <= PFH < 10^-6; SIL 4: 10^-8 <= PFH < 10^-7. The achieved SIL is determined by the hardware reliability (using reliability block diagrams and FMEA) and the software quality evidence (DO-178C compliance level). Students calculate the required SIL for their simulated PVSLR interlocking based on a tolerable hazard rate of 10^-6 fatalities per hour.

3.4 — DO-178C Software Quality Levels

DO-178C (analogous to IEC 62425 for railway) defines five software levels (A–E) by failure severity. For a safety-critical interlocking (failure could be catastrophic — Level A), requirements include: 100% statement coverage, 100% decision coverage, modified condition/decision coverage (MC/DC), independent verification of every requirement, and formal configuration management of every software artifact. Students assess their interlocking software against Level B (hazardous but not catastrophic) requirements as the most achievable in a capstone context.

Laboratory Investigation — Module 3

Experiment 3A — FPGA Interlocking Implementation (120 min)

Students implement the 4-route interlocking FSM in VHDL on the Xilinx Artix-7 FPGA. Required deliverables: (1) state transition diagram; (2) VHDL source code with comments; (3) testbench simulation waveform showing all state transitions including conflict detection; (4) synthesis report showing gate count, maximum clock frequency (timing closure), and resource utilization; (5) hardware demonstration on the actual O Scale layout with the FPGA controlling the signal LEDs and switch machine.

Experiment 3B — RTOS Task Scheduling Measurement (90 min)

Implement the task set from Table 3.2 on FreeRTOS running on the Raspberry Pi. Instrument each task with GPIO toggles that can be captured on the logic analyzer. Record: actual inter-arrival times (verify periodicity); actual execution times (compare to WCET estimates); any deadline misses (task did not complete within its period); response time to the highest-priority sensor polling task. Calculate actual CPU utilization from the logic analyzer trace. Compare to the theoretical RMS schedulability bound.

Experiment 3C — Fault Injection Testing (60 min)

Inject three categories of faults and document system response: (1) Hardware fault: disconnect one track occupancy sensor mid-operation. Does the interlocking fail safe (stop all signals) or fail dangerous (grant conflicting routes)? (2) Software fault: introduce a deliberate off-by-one error in the state transition logic. Does the testbench catch it? Does the hardware demonstrate it? (3) Timing fault: increase the PID task WCET by inserting a busy-wait loop until a deadline miss occurs. What happens to the interlocking response time? Document all faults, effects, detection methods, and recommended mitigations in an FMEA table.

Module 3 Consulting Report Section Requirements

- FPGA Architecture: block diagram of the interlocking system; state transition diagram for the 4-route interlocking; VHDL module hierarchy; synthesis report summary (gates, Fmax, resource utilization)
- RTOS Specification: task table with periods, WCETs, priorities; RMS schedulability analysis with utilization sum vs. bound; logic analyzer trace annotated with task boundaries; deadline miss analysis

- SIL Determination: tolerable hazard rate from risk analysis; required PFH calculated; target SIL stated with IEC 61508 reference; hardware reliability block diagram; achieved SIL estimate
- Software Safety Case: DO-178C level selected with justification; test coverage achieved (statement, decision, MC/DC — as applicable); fault injection test results; FMEA table for software faults; gap analysis vs. selected DO-178C level
- Professional Ethics Statement: one page — the engineer's professional responsibility when deploying safety-critical software; what obligations exist if a safety gap is discovered post-deployment; reference NSPE Canon 1 and IEC 61508 Clause 8

Assessment — Module 3

Criterion	4 – Exemplary	3 – Proficient	2 – Developing	1 – Beginning
FPGA Implementation	FSM correctly handles all states including conflict; VHDL synthesizes and meets timing closure; testbench covers all state transitions; hardware demonstrated on layout; synthesis report analyzed	FSM correct; VHDL synthesizes; testbench covers primary transitions; hardware demonstrated	FSM correct; VHDL synthesizes; testbench covers happy path only; no hardware demo	VHDL written but does not synthesize; no testbench; no hardware demo
RMS Schedulability	Utilization calculated for all tasks; sum compared to RMS bound; schedulability conclusion stated; logic analyzer trace confirms actual execution times match WCET estimates	Utilization calculated; RMS bound compared; schedulability stated; trace analyzed	Utilization calculated; RMS bound compared; trace not analyzed	Utilization calculated; RMS bound not applied; no trace analysis
SIL Determination	Tolerable hazard rate justified; PFH_required calculated; target SIL stated with IEC 61508 citation; reliability block diagram for hardware; achieved SIL estimated with calculation	THR justified; PFH calculated; SIL stated; reliability block diagram present	THR stated; PFH calculated; SIL stated; no reliability block diagram	SIL stated without derivation from tolerable hazard rate

Fault Injection FMEA	All 3 fault categories tested; fail-safe vs. fail-dangerous behavior documented; FMEA table complete with effect, detection, and mitigation for each fault; software fault detected by testbench confirmed	All 3 faults tested; fail-safe behavior documented; FMEA table with most fields	2 of 3 faults tested; fail-safe documented; FMEA table with effects only	1 fault tested; no systematic FMEA
Safety Ethics Statement	Clearly articulates post-deployment safety obligation; references NSPE Canon 1 by article; addresses whistleblower scenario; distinguishes professional from legal obligation; written at professional PE level	Canon 1 referenced; post-deployment obligation addressed; whistleblower mentioned	Professional obligation addressed; no Canon 1 citation; whistleblower not addressed	Obligation described generically; no professional code citation

MODULE 4

Communications & Network Engineering

Wireless Link Budget, CAN Bus Protocol, Cybersecurity Threat Modeling & IEC 62280

Duration	3 weeks (Weeks 10–12)
EE/CE Threads	Communications Engineering · Computer Networks · Cybersecurity · Protocol Design
ABET Outcomes	(1)(2)(3)(4)(6)(7) — ABET (4) addressed through cybersecurity ethics and responsible disclosure
Core Concepts	RF link budget, Friis transmission equation, Shannon-Hartley capacity theorem, CAN bus arbitration, DCC over IP, STRIDE threat model, attack surface analysis, IEC 62280 railway cybersecurity, defense-in-depth, penetration testing methodology, residual risk register
Math Required	dB arithmetic, Friis equation, Shannon capacity C=B*log2(1+SNR), probability of bit error (BER) vs. Eb/N0, queuing delay for CAN bus, cryptographic key size vs. security level
Standards Applied	IEC 62280 (Railway Communication Security); IEEE 802.11 (WiFi); CAN FD specification (ISO 11898); NIST Cybersecurity Framework; OWASP IoT Attack Surface
Consulting Report Section	Section 5: Communications & Network Security Architecture — Wireless System Design, CAN Bus Specification, Threat Model & Security Controls

Industry Context

Modern railroad communications systems are complex, layered, and increasingly vulnerable to cyberattack. Positive Train Control (PTC) uses 220 MHz licensed spectrum for train-to-wayside communications. Yard management systems use 2.4 GHz WiFi and 900 MHz mesh networks. DCC-over-IP (LCC — Layout Command Control, the next-generation DCC standard) routes DCC commands over Ethernet and WiFi. In December 2020, a security researcher demonstrated that legacy DCC radio systems used in large layout installations could be spoofed — a malicious actor could transmit locomotive commands from outside the building. IEC 62280 mandates cybersecurity risk assessment for all railway electronic systems. Senior engineers designing these systems must be fluent in both RF engineering and cybersecurity.

Theoretical Foundations

4.1 — RF Link Budget & Friis Transmission Equation

```
P_r(dBm) = P_t(dBm) + G_t(dBi) + G_r(dBi) - FSPL(dB) - L_misc(dB)
FSPL(dB) = 20*log10(4*pi*d*f/c)
```

Where P_r = received power; P_t = transmitted power; G_t, G_r = transmit/receive antenna gains; FSPL = free-space path loss; L_misc = miscellaneous losses (cable, connector, body shielding). Students calculate the link budget for a 2.4 GHz ESP32 wireless DCC controller at 10m range inside a building (add 10–15 dB penetration loss per wall).

4.2 — Shannon-Hartley Channel Capacity

```
C = B * log2(1 + S/N)   [bits/second]
```

Where B = bandwidth (Hz); S/N = signal-to-noise ratio (linear). For the measured receive power P_r and thermal noise floor N = kTB: S/N = P_r/N. Students calculate the maximum achievable data rate for their wireless link, compare to the DCC packet rate required (approximately 10 kbps for locomotive control), and determine the link margin — the excess SNR above the minimum required.

4.3 — CAN Bus Arbitration & Timing

CAN (Controller Area Network) uses bitwise non-destructive arbitration: the node transmitting the lowest CAN ID wins the bus. For a CAN bus at 1 Mbps with maximum propagation delay of 200 ns:

```
Maximum bus length = c*tau_prop/(2*1) ≈ 300m at 1 Mbps
```

Worst-case latency for a message with CAN ID N (N nodes contending):

```
L_worst = (N-1) * t_frame   where t_frame = 111 bit times at 1Mbps = 111 microseconds
```

Students verify the arbitration behavior using the logic analyzer: transmit two messages simultaneously from two nodes with different CAN IDs and observe which wins the bus.

4.4 — STRIDE Threat Modeling

STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) is a systematic threat identification framework from Microsoft Research. For each component of the DCC communications system, students apply STRIDE:

Component	Threat Type	Specific Threat Description	Proposed Mitigation
Wireless DCC controller	Spoofing	Attacker transmits locomotive commands on same WiFi channel	WPA3 encryption; MAC address filtering; SSID hiding
CAN bus	Tampering	Node injects malicious brake commands	CAN message authentication code (MAC); bus isolation
Web-based throttle	Elevation of Privilege	Attacker escalates from guest to admin role on DCC server	Role-based access control; session timeout; MFA
DCC booster	Denial of Service	Flood CAN bus to prevent legitimate commands reaching boosters	Priority queuing; rate limiting; watchdog timer
Track occupancy data	Information Disclosure	Attacker monitors sensor data to track locomotive positions	Encrypted telemetry channel; data minimization
Firmware update channel	Tampering	Attacker uploads malicious firmware to decoder	Code signing; secure boot; version rollback protection

Laboratory Investigation — Module 4

Experiment 4A — RF Link Budget Measurement (60 min)

Configure one ESP32 as a WiFi access point and a second as a client transmitting RSSI (received signal strength indicator) reports every 100ms. Measure RSSI at distances of 1, 3, 5, 10, 15, and 20 meters in the lab environment. Plot RSSI (dBm) vs. log(distance). Fit a path loss model: PL(d) = PL(d0) + 10*n*log10(d/d0) + X_sigma. Extract the path loss exponent n and shadow fading standard deviation sigma. Compare n to free-space value (n=2) and typical indoor value (n=3–4). Calculate the maximum reliable range for DCC control (minimum RSSI = -75 dBm for reliable WiFi at 1 Mbps).

Experiment 4B — CAN Bus Protocol Implementation (75 min)

Connect two MCP2515 CAN controllers (one per Raspberry Pi). Implement: (1) a DCC speed command message (CAN ID 0x001, data = speed_step, direction); (2) a sensor status broadcast (CAN ID 0x100, data = 8 sensor bits); (3) a higher-priority emergency stop (CAN ID 0x000, data = 0xFF). Verify arbitration: transmit ID 0x001 and ID 0x000 simultaneously; confirm ID 0x000 always wins. Measure message latency using logic analyzer timestamps. Verify that the emergency stop message always arrives within 2 ms of transmission (hard real-time requirement). Calculate bus utilization at the required message rates.

Experiment 4C — Penetration Test on Simulated DCC Network (90 min)

The instructor sets up a deliberately vulnerable simulated DCC WiFi controller (a Raspberry Pi running a basic HTTP throttle server with no authentication). Student teams conduct a structured penetration test using the OWASP IoT methodology:

6. Reconnaissance: use nmap to discover the target device; identify open ports; identify the HTTP server software version.
7. Vulnerability scanning: use nikto or similar tool to identify known web vulnerabilities; identify missing authentication on the throttle endpoint.
8. Exploitation: send a raw HTTP POST request to the throttle endpoint with a crafted speed command; verify the locomotive responds to the unauthorized command.
9. Privilege escalation: attempt to access the admin configuration page; document whether default credentials are in use.
10. Document all findings in a penetration test report using the PTES (Penetration Testing Execution Standard) format: scope, findings, severity (CVSS score), evidence, and remediation recommendation.

Ethical Boundary: All penetration testing in this lab is conducted on equipment owned by the course and within the explicit permission scope defined by the instructor. Students sign a Rules of Engagement document before any testing begins. Unauthorized penetration testing of real systems — including real railroad networks — is a federal crime under the Computer Fraud and Abuse Act (18 U.S.C. § 1030). The professional and legal obligation to obtain written authorization before any security testing is non-negotiable and will be assessed as part of the Module 4 ethics component.

Module 4 Consulting Report Section Requirements

- Wireless Network Architecture: system diagram showing all wireless nodes; link budget calculation for each critical link; coverage map with minimum RSSI contours; channel plan to minimize co-channel interference
- CAN Bus Specification: message catalog (ID, data fields, period, priority for each message type); bus utilization calculation; worst-case latency analysis; emergency stop latency verification
- STRIDE Threat Model: completed threat table for all system components; attack surface diagram; threat severity rated by CVSS score; residual risk register after mitigations
- IEC 62280 Gap Analysis: completed checklist against IEC 62280 Clause 5 (security requirements for railway communication systems); non-conformances identified; remediation plan with priority and estimated effort
- Penetration Test Report: scope and rules of engagement; findings in PTES format with CVSS scores; remediation recommendations; responsible disclosure process described

Assessment — Module 4

Criterion	4 – Exemplary	3 – Proficient	2 – Developing	1 – Beginning
Link Budget Analysis	Friis equation applied with all terms; path loss model fitted to measured data with n and sigma extracted; maximum range calculated; coverage map conceptualized; compared to IEEE 802.11 sensitivity specification	Friis applied; path loss model fitted; maximum range calculated; no coverage map	Friis applied; RSSI measured at multiple distances; maximum range estimated	RSSI measured; Friis not applied; range estimated empirically
CAN Bus Implementation	All 3 message types implemented; arbitration verified experimentally; emergency stop latency measured and meets 2ms spec; bus utilization calculated; logic analyzer traces annotated	All 3 messages implemented; arbitration verified; latency measured; utilization calculated	2 of 3 messages; arbitration verified; latency measured; utilization estimated	1 message type; no arbitration verification; no latency measurement
STRIDE Threat Model	All 6 STRIDE categories applied to all	All 6 STRIDE categories applied to	STRIDE applied; threats identified; CVSS	STRIDE categories listed without specific

	major components; threats are specific and credible; CVSS scores assigned; residual risk register populated after mitigations; IEC 62280 gap analysis completed	primary components; CVSS scores assigned; residual risk register present	not calculated; no IEC 62280 analysis	threats; no CVSS; no residual risk
Penetration Test Report	Report follows PTES format; all findings include CVSS score and evidence; remediation recommendations are specific; responsible disclosure process stated; rules of engagement documented	PTES format used; most findings have CVSS and evidence; remediation recommendations present	Findings documented informally; CVSS for primary finding; remediation recommendations	Penetration test performed; findings listed without CVSS, evidence, or remediation
Cybersecurity Ethics	Rules of engagement signed and included in appendix; Computer Fraud and Abuse Act reference with specific statute; responsible disclosure obligation explained; distinction between authorized testing and unauthorized access is precise and legally accurate	ROE signed; CFAA referenced; responsible disclosure explained	ROE signed; CFAA mentioned; responsible disclosure addressed generally	Ethical boundary acknowledged but CFAA not cited; no ROE

MODULE 5

Systems Integration & Verification

Hardware-in-the-Loop Testing, Fault Injection, Coverage Analysis & Formal V&V

Duration	2 weeks (Weeks 13–14)
EE/CE Threads	Systems Engineering · Verification & Validation · Test Engineering · Quality Assurance
ABET Outcomes	(1)(2)(3)(6) — V&V is the bridge between design and professional delivery
Core Concepts	Hardware-in-the-loop (HIL) test architecture, test coverage matrix, requirements traceability matrix (RTM), non-conformance report (NCR), regression testing, formal methods (model checking with SPIN or NuSMV — conceptual), system-level performance envelope, acceptance testing
Standards Applied	IEEE 829 (Software Test Documentation); MIL-STD-882E (System Safety); RTCA DO-160 (Environmental Conditions — analogous for EMC/vibration testing)
Consulting Report Section	Section 6: Verification & Validation Report — Test Architecture, Coverage Evidence, Non-Conformance Register & System Acceptance Statement

Theory — Verification vs. Validation

Verification answers: "Did we build the system right?" (Does it conform to the specification?) Validation answers: "Did we build the right system?" (Does it meet the stakeholder's actual need?) Both are required for a professional engineering deliverable. In safety-critical systems, the distinction is formalized in IEC 61508 Clause 7 (V&V) and DO-178C Section 6 (software verification).

5.1 — Requirements Traceability Matrix (RTM)

Every system requirement must be traceable to: (1) its source (client brief, standard, or derived requirement); (2) the design element that implements it; (3) the test case that verifies it; (4) the test result. The RTM is the central document of the V&V process. A requirement without a test case is unverified. An unverified requirement is a professional and legal liability.

5.2 — Test Coverage Analysis

Coverage metrics quantify the completeness of testing:

- Requirements coverage: percentage of requirements with at least one passing test case
- Statement coverage: percentage of software statements executed by the test suite
- Decision coverage: percentage of Boolean outcomes (true/false) exercised
- MC/DC (Modified Condition/Decision Coverage): each condition in a decision independently affects the decision outcome — required for DO-178C Level A/B

Students calculate requirements coverage from their RTM and statement/decision coverage using a Python coverage tool (coverage.py) on their RTOS and Kalman filter code.

5.3 — Hardware-in-the-Loop (HIL) Architecture

HIL testing replaces physical plant components with real-time simulation, allowing the actual embedded controller to be tested against a simulated environment without risk to physical equipment. For the DCC interlocking: the FPGA controller under test receives simulated sensor inputs (track occupancy, switch position) from a Raspberry Pi running a track simulation model. The FPGA outputs (signal aspects, switch commands) are captured and verified against expected outputs. This allows fault injection — injecting sensor failures that would be difficult or dangerous to create on real hardware.

Laboratory Investigation — Module 5

Experiment 5A — Build the Requirements Traceability Matrix (60 min)

Teams compile their complete RTM covering all four previous modules. For each requirement: trace to source; trace to design element (with section number in the consulting report); assign a test case ID; run the test; record pass/fail. Calculate requirements coverage. Identify any untested requirements and either write a new test or justify why the requirement cannot be tested (with risk assessment).

Experiment 5B — HIL Test Execution (90 min)

Configure the HIL test setup: Raspberry Pi (simulation) feeds sensor signals via GPIO to the FPGA (interlocking controller). Run the complete test suite against the HIL setup including: normal operations (all routes granted correctly); conflict scenarios (all conflicts locked out); sensor failures (occupancy sensor stuck-high, stuck-low); power interruption and restart (does the interlocking return to a safe state?). Record all results in the test log. Any failure generates a Non-Conformance Report (NCR) documenting: description of failure, expected vs. actual behavior, severity (critical/major/minor), root cause analysis, and corrective action.

Experiment 5C — System Performance Envelope Test (60 min)

Define the system performance envelope: maximum train speed, minimum headway, maximum grade, minimum track circuit resistance, maximum ambient temperature. Test the system at the boundary of each parameter. Record: does performance degrade gracefully or fail abruptly? Plot performance metrics vs. each boundary parameter. Identify the parameter with the steepest performance cliff — this is the system's most sensitive dimension and must be highlighted in the consulting report as a key operational constraint.

Experiment 5D — Regression Test Suite (30 min)

After implementing any corrective actions from 5B NCRs: re-run the complete test suite. Verify no new failures have been introduced (regression). Calculate the final requirements coverage percentage. Sign the Acceptance Test Report: a formal document stating that the system has been tested, all critical NCRs have been resolved, and the system is ready for delivery to the client. This document is signed by the team's designated Engineer of Record.

Assessment — Module 5

Criterion	4 – Exemplary	3 – Proficient	2 – Developing	1 – Beginning
Requirements Traceability Matrix	RTM covers all stated requirements from all 4 modules; every requirement traced to design element and test case; requirements coverage calculated; untested requirements analyzed with risk assessment	RTM covers primary requirements; coverage calculated; most requirements traced; untested requirements listed	RTM covers primary requirements; most traced; coverage estimated; untested not analyzed	RTM present but incomplete; coverage not calculated; several requirements without test cases
HIL Test Execution & NCR	HIL setup configured and operational; all test cases executed; failures documented with complete NCRs (description, expected vs. actual, severity, root cause, corrective action); NCR log submitted	HIL setup operational; all tests executed; failures documented with most NCR fields; NCR log submitted	HIL setup operational; primary tests executed; failures noted without complete NCR fields	HIL setup attempted; some tests run; failures noted without NCR format
Performance Envelope	All boundary parameters tested; pass/fail recorded at each boundary; most sensitive parameter identified with quantitative evidence; performance cliff documented	Most boundaries tested; most sensitive parameter identified; performance cliff noted	3+ boundaries tested; most sensitive parameter estimated; no performance cliff analysis	2 or fewer boundaries tested; no sensitivity ranking
Regression Testing	Complete regression suite run after all corrective actions; zero new failures introduced;	Regression run; zero new failures; coverage calculated; Acceptance Test Report signed	Regression run; one new failure (with NCR); coverage calculated; report signed	Regression not run; or new failures not documented

	requirements coverage final value calculated; Acceptance Test Report signed by EOR			
Test Documentation Quality	Test log in IEEE 829 format: test ID, test case, input, expected output, actual output, pass/fail, date, tester; all figures from HIL setup captured and labeled; acceptance report professionally formatted	IEEE 829 format used; most fields complete; figures present; acceptance report present	Test log present; informal format; most fields complete; figures unlabeled	Test log is notes; no IEEE 829 structure; no figures; no acceptance report

WEEK 15 · CAPSTONE DELIVERY

Professional Consulting Report & Client Presentation

Pocono Valley Short Line Railroad — System Design Report

Deliverable	Complete System Design Report — professional engineering consulting report format
Minimum Length	50 pages of technical content plus appendices (raw data, code listings, schematics, test logs)
Presentation	30-minute client presentation + 15-minute Q&A panel (includes at least one practicing EE/PE and one non-engineer "board member")
Engineer of Record	One student per team designated as EOR; signs the cover page professional certification; role rotated from Module 3 designation
Grading Weight	Module Report Sections (40%) + Integration & Coherence of Final Report (25%) + Client Presentation (20%) + Individual Reflection (15%)

Final Report Structure

Cover Page & Professional Certification

Report title; client name and address; engineering firm name (team name); date of submission; revision number; EOR name, degree, and professional certification statement: "I certify that this report represents my team's professional engineering judgment based on the evidence gathered and analyzed during this engagement. I accept professional responsibility for the findings and recommendations herein." Signed and dated by the EOR.

Executive Summary (2 pages maximum)

Written for a non-engineer reader — the PVSLR Board of Directors. States: what was assessed, the three most important findings, the recommended capital investment, the estimated total project cost, and the risk of not acting. No equations, no jargon. Every technical claim must be defensible from the body of the report.

Section 1 — Project Background & System Requirements

Client brief restated in engineering language. Formal requirements specification — each requirement numbered, measurable, and traceable. System architecture overview block diagram. Constraints and assumptions table. Regulatory environment (FRA, IEEE, IEC standards that govern the work).

Section 2 — Traction Power System Design (Module 1)

Full content from Module 1 consulting report section, refined and integrated into the final report context. Must include: one-line power diagram; all measurements with instrument uncertainty; IEEE 519 and

FCC compliance assessment; filter and ferrite mitigation specifications; arc flash PPE specification; power budget.

Section 3 — Adaptive Speed Control System (Module 2)

Full content from Module 2 consulting report section. Must include: motor transfer function with experimental validation; PID design with Bode plot stability margins; Kalman filter specification with Q and R matrices; grade rejection performance; digital implementation specification.

Section 4 — Signal Interlocking System (Module 3)

Full content from Module 3 consulting report section. Must include: FPGA architecture and FSM specification; RTOS task schedule with RMS analysis; SIL determination; DO-178C compliance level with evidence; fault injection FMEA; professional ethics statement.

Section 5 — Communications & Network Security (Module 4)

Full content from Module 4 consulting report section. Must include: wireless network architecture with link budgets; CAN bus specification and latency analysis; STRIDE threat model; IEC 62280 gap analysis; penetration test findings; residual risk register.

Section 6 — Verification & Validation (Module 5)

Full content from Module 5 consulting report section. Must include: requirements traceability matrix (as appendix); HIL test results summary; NCR register; performance envelope; acceptance test statement signed by EOR.

Section 7 — Integrated Risk Register

Consolidated risk register combining all residual risks identified in Sections 2–6. Each risk: ID, description, source section, likelihood (1–5), consequence (1–5), risk score, owner, mitigation status, residual risk score. Top 5 risks highlighted for board attention.

Section 8 — Capital Investment Recommendation

Cost estimate for all recommended improvements (order-of-magnitude, ±30%). Prioritized implementation schedule (immediate, 6-month, 12-month, 3-year). NPV analysis for the top three investment alternatives using a 10-year planning horizon at 8% discount rate. Recommended alternative with full justification. Risk of deferral — what happens if no action is taken.

Appendices

- Appendix A — Raw Measurement Data (all experimental data tables)
- Appendix B — VHDL Source Code (interlocking FSM with comments)
- Appendix C — Software Source Code (PID, Kalman filter, CAN bus driver, with inline documentation)

- Appendix D — Requirements Traceability Matrix (complete)
- Appendix E — Test Logs (all Module 5 test records in IEEE 829 format)
- Appendix F — Non-Conformance Reports (all NCRs with closure status)
- Appendix G — References (IEEE/IEC standards, technical papers, cited per IEEE citation format)

Client Presentation Requirements

The 30-minute presentation is structured as a professional engineering briefing to a client board, not as an academic seminar. Required structure:

11. Opening (2 min): team introduction; scope of engagement; one-sentence summary of key finding
12. Power & Control Systems (6 min): most critical finding from Sections 2–3; one quantitative result; recommended action
13. Safety & Cybersecurity (6 min): SIL determination result; top 3 cybersecurity threats with CVSS scores; recommended mitigations
14. Verification & Risk (6 min): requirements coverage achieved; top 3 residual risks; risk register summary
15. Investment Recommendation (6 min): recommended alternative with NPV; implementation timeline; consequences of deferral
16. Q&A (15 min): panel questions from practicing EE/PE and non-engineer board member

> **Presentation Evaluation Note:** The non-engineer board member will evaluate whether the team can communicate technical findings in terms a business decision-maker can act on. The practicing EE/PE will evaluate technical accuracy and professional judgment. Both evaluations carry equal weight. A team that can only communicate to engineers has not met ABET Outcome (3).

Final Capstone Assessment

Criterion	4 – Exemplary	3 – Proficient	2 – Developing	1 – Beginning
Technical Accuracy & Depth	All six sections technically correct with derivations; all measurements include instrument uncertainty; all code annotated; all standards correctly applied and cited by clause number; findings independently verifiable from	All sections correct; most standards cited by clause; uncertainties reported; code annotated	All sections present; 1–2 technical errors; standards cited generically; uncertainties missing	One or more sections with significant technical errors or missing

	appendices			
Integration & Coherence	Sections are internally consistent (e.g., power budget from M1 matches load assumed in M2; SIL from M3 matches risk register in M7); integrated risk register coherently combines all section risks; investment recommendation is grounded in all six sections	Sections mostly consistent; risk register integrates 4+ sections; investment grounded in most sections	Sections independently correct but inconsistencies at interfaces; risk register partially integrated	Sections appear written independently; no cross-referencing; risk register not integrated
Executive Summary Quality	Written for non-engineer reader; no unexplained jargon; three most important findings clearly stated; investment recommendation with cost and timeline; risk of no action stated; all claims traceable to body of report	Non-engineer appropriate; three findings stated; recommendation with cost; deferral risk mentioned	Written for engineer audience; findings stated; recommendation present; deferral risk not addressed	Executive summary is a technical abstract; not appropriate for board-level audience
Client Presentation	Time managed within 30 min; non-engineer questions answered without jargon; PE questions answered with specific reference to calculations and standards; all required presentation sections covered; EOR speaks with professional authority	Time managed; most PE questions answered with specifics; most non-engineer questions accessible; all sections covered	Time managed; PE questions partially answered; non-engineer communication inconsistent; all sections covered	Over or under time by >5 min; PE questions not answered specifically; sections missing
Professional	EOR certification	Certification	Certification	Certification

Certification & Ethics	statement present, specific, and signed; professional responsibility acknowledged for all findings; limitations of the engagement stated; recommendations include appropriate caveats; ethics statement from M3 integrated	signed; responsibility acknowledged; limitations stated; caveats present	signed; responsibility acknowledged; limitations stated; caveats missing	present but generic; limitations not stated; no caveats on recommendations

Appendix A — Key Equations & Constants by Module

Module	Concept	Formula / Standard
1	Fourier series (square wave)	`v(t) = (4A/pi)*[sin(w0*t) + (1/3)sin(3w0*t) + ...]`
1	Total Harmonic Distortion	`THD = sqrt(V2^2+V3^2+...)/V1 * 100%`
1	Characteristic Impedance	`Z0 = sqrt((R+jwL)/(G+jwC))`
1	Free-Space Path Loss	`FSPL(dB) = 20*log10(4*pi*d*f/c)`
1	Arc Flash Incident Energy	`E = 4.184*Cf*En*(t/0.2)*(610^x/D^x) [cal/cm^2]`
2	DC Motor Transfer Function	`G(s) = Km/(tau_m*s + 1)`
2	PID Controller (continuous)	`C(s) = Kp + Ki/s + Kd*s`
2	Tustin Discretization	`s = 2/T*(z-1)/(z+1)`
2	Kalman Predict Step	`x[-] = F*x[+], P[-] = F*P[+]*F' + Q`
2	Kalman Update Step	`K = P[-]*H'*(H*P[-]*H'+R)^-1; x[+] = x[-] +K*(z-H*x[-])`
3	RMS Schedulability Test	`sum(Ci/Ti) <= n*(2^(1/n)-1)  [Liu & Layland 1973]`
3	SIL from PFH	`SIL1: 1e-5>PFH>=1e-4; SIL2: 1e-6; SIL3: 1e-7; SIL4: 1e-8`
3	Fault Tree AND Gate	`P(top) = P(A)*P(B)`
3	Fault Tree OR Gate	`P(top) = 1-(1-P(A))*(1-P(B))`
4	Friis Transmission	`Pr(dBm) = Pt + Gt + Gr - FSPL - L_misc`
4	Shannon Capacity	`C = B*log2(1 + S/N) [bps]`
4	CAN Bus Worst-Case Latency	`L_worst = (N-1)*t_frame where t_frame=111 bits at 1Mbps`
5	Requirements Coverage	`RC = (Tested Requirements)/(Total Requirements)*100%`
5	Decision Coverage	`DC = (Outcomes Tested)/(Total Boolean Outcomes)*100%`

Appendix B — O Scale Electrical Reference Data

Parameter	O Scale Specification	Applicable Standard
DCC track voltage (nominal)	14.5–16V AC RMS	DCC S-9.1

DCC "1" bit half-period	58 ± 3 µs	DCC S-9.1
DCC "0" bit half-period	100 µs (min 100, max 10,000)	DCC S-9.1
DCC preamble bits (minimum)	14 "1" bits	DCC S-9.1
Booster short circuit trip time	< 100 ms	DCC RP-9.1.2
Track gauge (O Scale)	1.25 inches (31.75 mm)	DCC S-1.2
Scale ratio	1:48	DCC S-1.2
Typical loco current draw	0.5–1.5A (decoder dependent)	Decoder datasheet
DCC fundamental frequency (typical)	4–8 kHz	DCC S-9.1 derived
Maximum recommended bus wire	14 AWG for main bus	DCC RP-9.1.1
Booster isolation requirement	Each power district fused separately	DCC RP-9.1.2
LCC (Layout Command Control)	OpenLCB / CAN-based, 125 kbps	DCC S-9.7

Appendix C — IEEE & IEC Standards Referenced

- DCC S-9.1: DCC Standard for Digital Command Control
- DCC S-9.7: Layout Command Control (LCC/OpenLCB)
- IEEE 519-2022: Harmonic Control in Electric Power Systems
- IEEE 829-2008: Standard for Software and System Test Documentation
- IEEE 1076-2019: VHDL Language Reference Manual
- IEEE 754-2019: Standard for Floating-Point Arithmetic
- IEC 61508:2010: Functional Safety of Electrical/Electronic/Programmable Safety-Related Systems (Parts 1–7)
- IEC 62280:2014: Railway Applications — Communication, Signalling and Processing Systems — Security for Railway Communication Systems
- IEC 62425:2007: Railway Applications — Communication, Signalling and Processing Systems — Safety Related Electronic Systems for Signalling
- NFPA 70E-2021: Standard for Electrical Safety in the Workplace
- FCC 47 CFR Part 15: Radio Frequency Devices (unintentional radiator limits)
- ISO 11898:2015: Road Vehicles — Controller Area Network (CAN) — Parts 1 & 2
- NIST SP 800-30 Rev 1: Guide for Conducting Risk Assessments (cybersecurity)
- RTCA DO-178C: Software Considerations in Airborne Systems (analogous to railway practice)
- PTES: Penetration Testing Execution Standard — pentest-standard.org
- 18 U.S.C. § 1030: Computer Fraud and Abuse Act (cybersecurity legal boundary)

Appendix D — Software Tools

Tool	Module(s)	Purpose & Access
Xilinx Vivado (WebPACK free)	3	FPGA synthesis, simulation, timing analysis — xilinx.com/vivado
ModelSim / Questa (free starter)	3	VHDL simulation and testbench execution
MATLAB + Simulink (student)	2,5	Control system design, Bode plots, Kalman filter simulation
Python + NumPy + SciPy	2,4,5	Kalman filter, FFT analysis, Monte Carlo, coverage analysis
coverage.py	3,5	Python statement and decision coverage measurement — coverage.readthedocs.io
GNU Radio + RTL-SDR	1	Software-defined radio for EMI spectrum survey — gnuradio.org
SDR# (SDRsharp)	1	Windows-based spectrum analyzer UI for RTL-SDR
Saleae Logic 2	3,4	Logic analyzer with CAN, SPI, UART protocol decode — saleae.com
Wireshark	4	Network packet capture and analysis — wireshark.org
nmap	4	Network discovery and port scanning (for authorized pentest only)
nikto	4	Web server vulnerability scanner (for authorized pentest only)
JMRI (Java Model Railroad Interface)	1,2	DCC decoder programming, layout automation — jmri.org
FreeRTOS	3	Real-time operating system for embedded experiments — freertos.org
Zephyr RTOS (alternative)	3	Linux Foundation RTOS with strong safety pedigree — zephyrproject.org
SkyCiv (free tier)	Reference	Structural analysis reference (cross-module context)
