

University of Wales Trinity Saint David

Wales Institute of Science and Art



Prifysgol Cymru

Y Drindod Dewi Sant

University of Wales

Trinity Saint David

Electronic circuit testing and Applications

Vehicle Electronics

Jerico Gumapos

2410103

19/04/2026

Contents

1	Task 3	1
1.1	Scope Time Division Calculations (6)	1
1.2	Function Generator output square wave (6)	1
1.3	Capacitor charge and discharge wave marked at correct points. (6)	1
1.4	Basic Capacitor Calculations (6)	2
1.5	Capacitor discharge table (5)	2
1.6	Plot log(V) Gradient (5)	2
1.7	Gradient Calculations and Compare(8)	3
1.7.1	Gradient Calculations	3
1.7.2	Comparison table	3
1.8	Capacitor Uses (5)	3
1.8.1	Other use of Capacitors	4
1.9	Inaccuracies Question (4)	4
1.10	Risk Question (10)	4
2	References	6

1 Task 3

1.1 Scope Time Division Calculations (6)

No. of divisions (Tdiv) = 10

Total time of one full cycle = 40τ

Time/div = $40\tau/10 = 4\tau$

1.2 Function Generator output square wave (6)

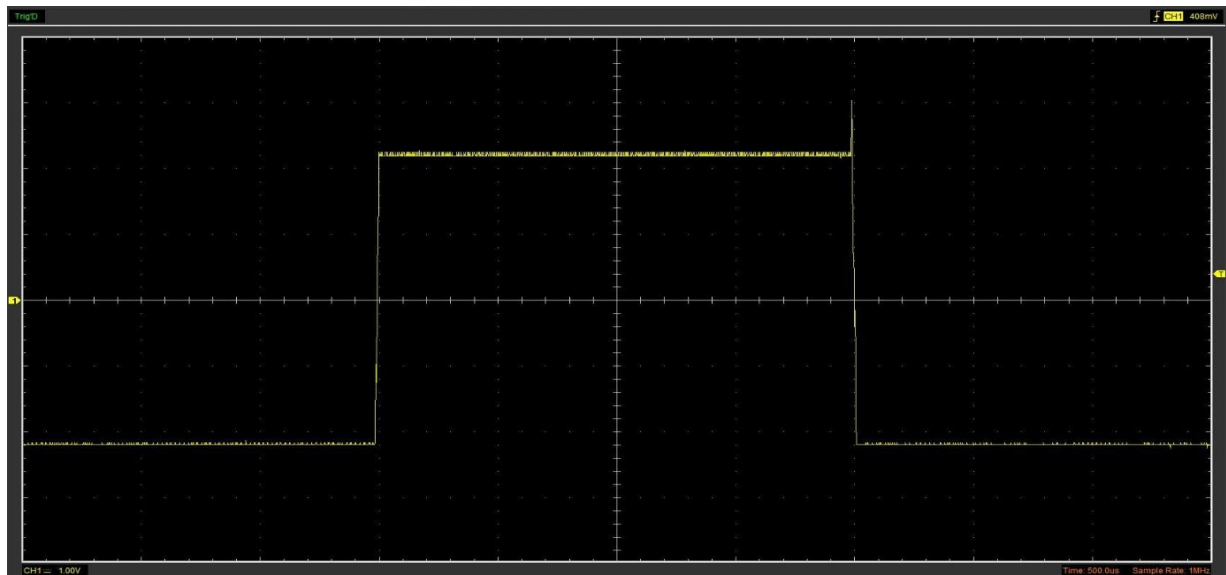


Figure 1: Output square wave

1.3 Capacitor charge and discharge wave marked at correct points. (6)

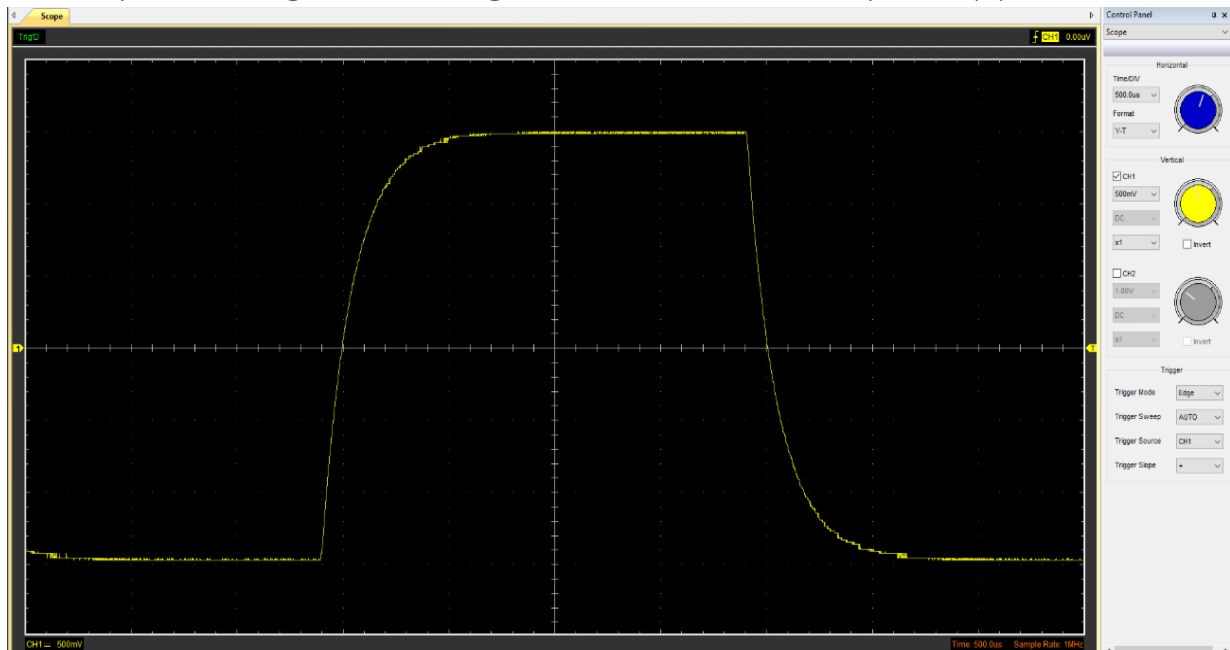


Figure 1.2 Capacitor charge and discharge wave.

1.4 Basic Capacitor Calculations (6)

$$\tau = RC$$

rearranging for capacitance: $C = \tau/R$

$$C = 1.54 \times 10^{-4} / 100$$

1.5 Capacitor discharge table (5)

Time (s)	Voltage (V)	ln (V)	dy = y2 – y1 dy = ln(V)2-ln(V)1	dx = x2- x1 dx = Time2 – Time1	dy/dx
0.00280	3.00	1.10	x	x	x
0.00284	2.56	0.94	-0.16	4×10^{-5}	-4000
0.00288	2.01	0.70	-0.24	4×10^{-5}	-6000
0.00292	1.58	0.46	-0.24	4×10^{-5}	-6000
0.00296	1.25	0.22	-0.24	4×10^{-5}	-6000
0.00300	0.95	-0.05	-0.27	4×10^{-5}	-6750
0.00304	0.71	-0.34	-0.29	4×10^{-5}	-7250
0.00308	0.52	-0.66	-0.32	4×10^{-5}	-8000
0.00312	0.37	-1.00	-0.34	4×10^{-5}	-8500
0.00316	0.30	-1.22	-0.22	4×10^{-5}	-5500

1.6 Plot log(V) Gradient (5)

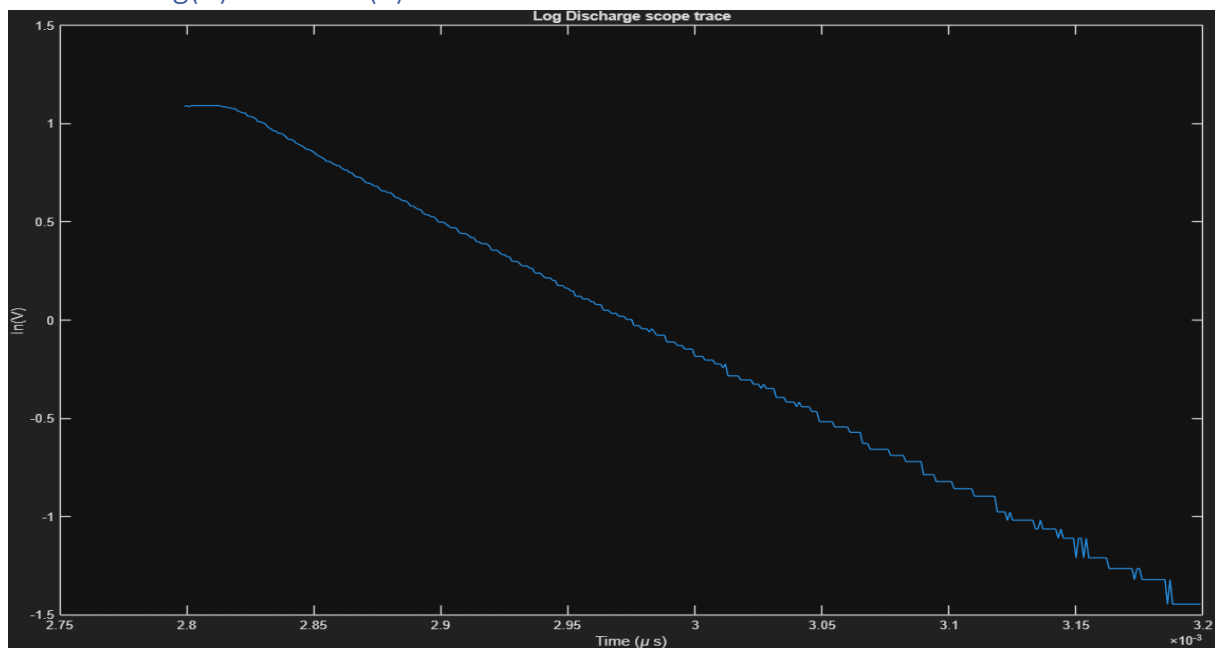
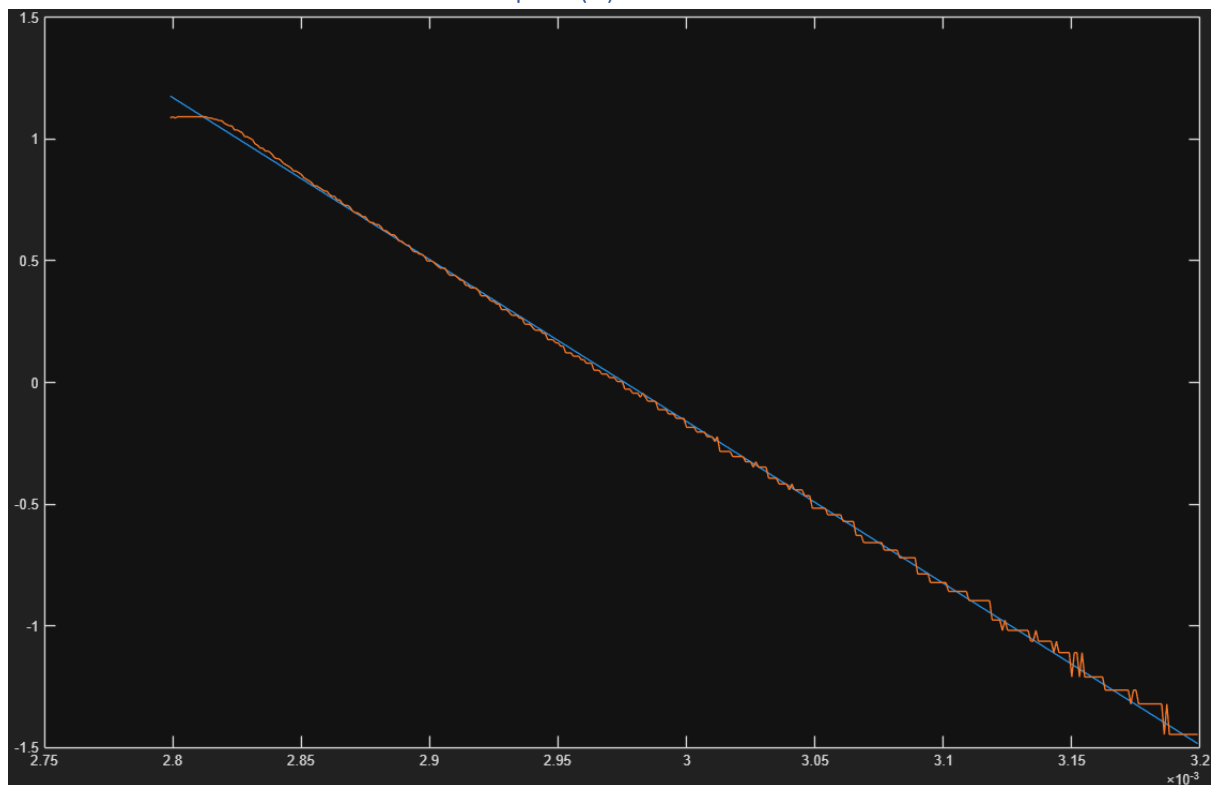


Figure 1.3 log(V) against time (μs)

1.7 Gradient Calculations and Compare(8)



1.7.1 Gradient Calculations

Mean gradient = $-6.44 \times 10^3 \text{ s}^{-1}$

$$= 1.55 \times 10^{-4} \text{ s}$$

$$= 1.55 \times 10^{-4} \text{ s/100}$$

1.7.2 Comparison table

	Capacitance	Delta	Percentage difference
Actual	1 μF	x	X
Marker Calculation	1.54 μF	0.54 μF	54%
Gradient Calculation	1.55 μF	0.55 μF	55%

1.8 Capacitor Uses (5)

A notable use of capacitors within automotive applications is within an alternator. The alternator generates alternating current later then converted into direct current by the use of a rectifier diode so it can supply charge to the battery and other electrical systems. However, within the rectified output there is small fluctuations referred to as ripples, these ripples can be monitored by capacitors smoothening the output.

When the rectified voltage rises to a peak, the capacitor stores the excess energy. As the voltage begins to drop, the capacitor discharges, releasing it stored energy back into the circuit. This

continuous charging and discharging reduces the ripple effect and produces a smooth direct current supply. (Kaiser, 2012)

1.8.1 Other use of Capacitors

- Start-stop systems
- Regenerative braking systems
- Ignition systems
- Backup power for safety systems (electronic control units, airbags, alarm etc.)

1.9 Inaccuracies Question (4)

The calculated capacitance values significantly differ from the actual value, main reason could possibly be the limited resolution of the oscilloscope. Also, component tolerances of the resistor and capacitor can factor into the overall inaccuracy.

1.10 Risk Question (10)

The controller area network (CAN) bus system allows various electronic devices within the vehicle to communicate with one another, amalgamating electronic control units (ECU) such as anti-lock braking systems, airbag control units and infotainment control unit etc without a central computer. Unfortunately, this system lacks built in security features making it vulnerable to cyberattacks such as malwares, denial of service and unauthorized access (David Ward, 2021) There are various strategies to mitigate cybersecurity attacks.

ISO/SAE 21434 addresses vehicle cybersecurity through categories to ensure the threats are evaluated thoroughly, modern vehicles have multiple cybersecurity entry points that being through the on-board diagnostic port, the infotainment system keyless entry, the previously stated systems can expose the internal CAN bus to be attacked.

The first method is a algorithm being advanced encryption standard (AES) this method encrypts messages exchanged between the ECUs by converting plain text into ciphertext so that the information is difficult to read or be tampered with by an unauthorized device. Within the CAN bus system, AES is applied to prevent eavesdropping and message spoofing. In addition to this AES also prevents physical attack protecting keyless entry by encrypting the communication between the vehicle and key fob preventing theft. (Apvrille, 2010)

Furthermore, another method to safeguard the vehicle's CAN bus system is CAN frame authentication this method ensures that the messages being communicated in the CAN bus are genuine and not tampered, it is added at a higher layer to protect against attacks like spoofing and replay but unfortunately with this method CAN traffic is still exposed to reverse engineering,

attackers can read all messages, data values like rpm, speed but cannot alter without the key. (Aliwa, 2021)

Another important strategy to mitigate cyberattacks is network segmentation a strategy outlined in ISO/SAE 21434 an innovative framework proposed to mitigate critical vulnerabilities by separating critical systems such as the steering and braking from non-critical systems such as the infotainment system this method is effective as the attacker is limited to how they navigate around the system, instead of having a large network where all electronic systems communicate they are divided into separate domains. (Castiglione, 2026)

Lastly, another strategy to mitigate cybersecurity breach is intrusion detection system. It is used to monitor traffic within the CAN bus system by identifying abnormal and malicious behaviour in live event, this can be a third-party protection feature on top of the authentication or segmentation in case they've been bypassed. (Lokman, 2019)

2 References

Aliwa, E. (2021). *Cyberattacks and countermeasures in vehicle networks*.

Apvrille, L. (2010). *Secure on-board electronics network architecture*.

Castiglione, A. (2026). Securing in-vehicle communications through network segmentation.

David Ward, P. W. (2021). *Automotive cybersecurity*. SAE international.

Kaiser, C. J. (2012). *The Capacitor Handbook*. Cletus J. Kaiser.

Lokman, S.-F. (2019). Intrusion detection system for automotive CAN bus system.