

University of Wales Trinity Saint David

Wales Institute of Science and Art



Prifysgol Cymru

Y Drindod Dewi Sant

University of Wales

Trinity Saint David

Vehicle Electronics

Electronic Circuits Testing and Applications ACHA4031

Ryan Hunt

2405213

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)	2
1.4	Basic Capacitor Calculations (6)	2
1.5	Capacitor discharge table (5)	3
1.6	Plot log(V) Gradient (5)	4
1.7	Gradient Calculations and Compare (8)	4
1.7.1	Gradient Calculations	4
1.7.2	Comparison table	4
1.8	Capacitor Uses (5)	4
1.9	Inaccuracies Question (4)	6
1.10	Risk Question (10)	6
2	References	8
Figure 1 - Square wave generated by the function generator		1
Figure 2 - Capacitor wave marked at 66% charge		2
Figure 3- Capacitor wave marked at 33% discharge		2
Figure 4 - Natural Log of Voltage plotted against time from excel calculations		4
Figure 5 - MR2 SW20 Headlight Control unit Circuit, Highlighting the capacitors being modified (Hrouda, 2023)		5
Figure 6 - Capacitor Stabilising Incoming Voltage (Huang et al., 2024)		5
Table 1 – 10 selected data points		3
Table 2- Capacitor Discharge Table		3
Table 4 - Comparison of expected results with recorded results		4

1 Task 3

1.1 Scope Time Division Calculations (6)

Capacitance, C (measured in Farads) = $1\mu\text{F}$

Resistance, $R = 100\Omega$

Wave frequency = 250 Hz

Wave period = $1/f = 0.004$

Time constant, $\tau = R \times C$

Number of time divisions = Wave frequency = $0.004/250 = 16\mu\text{s}$

1.2 Function Generator output square wave (6)

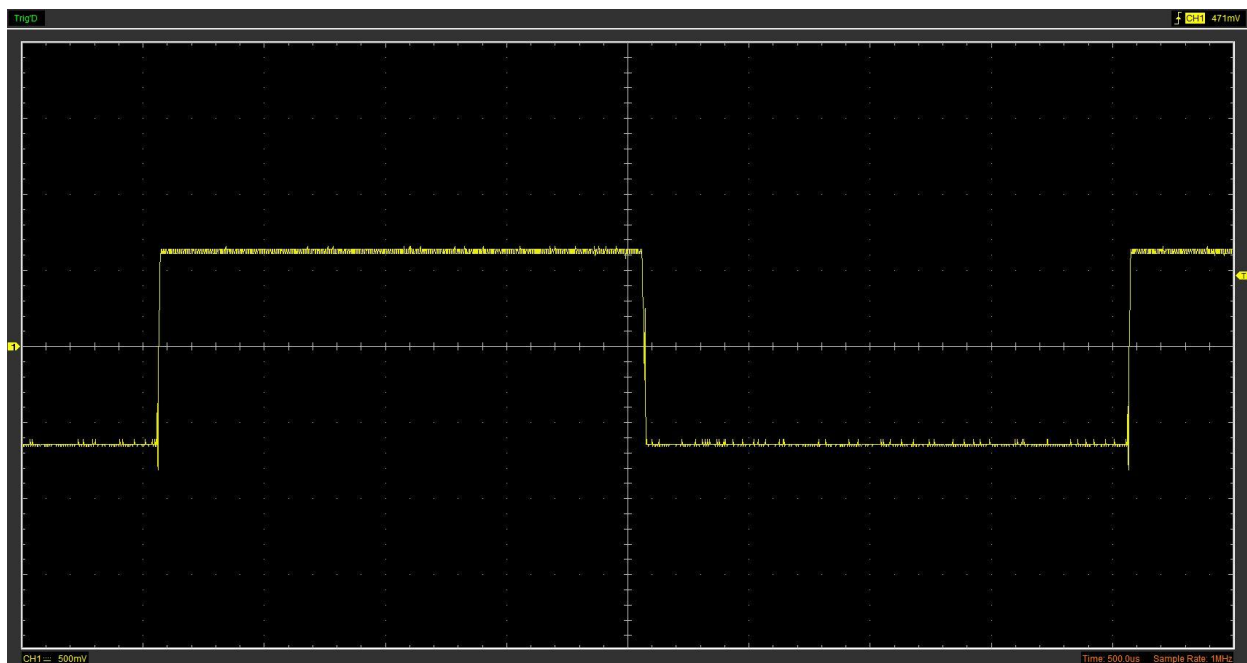


Figure 1 - Square wave generated by the function generator

CH1 = 500 mV

Time = $500\text{ }\mu\text{s}$

Sample Rate = 1 MHz

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

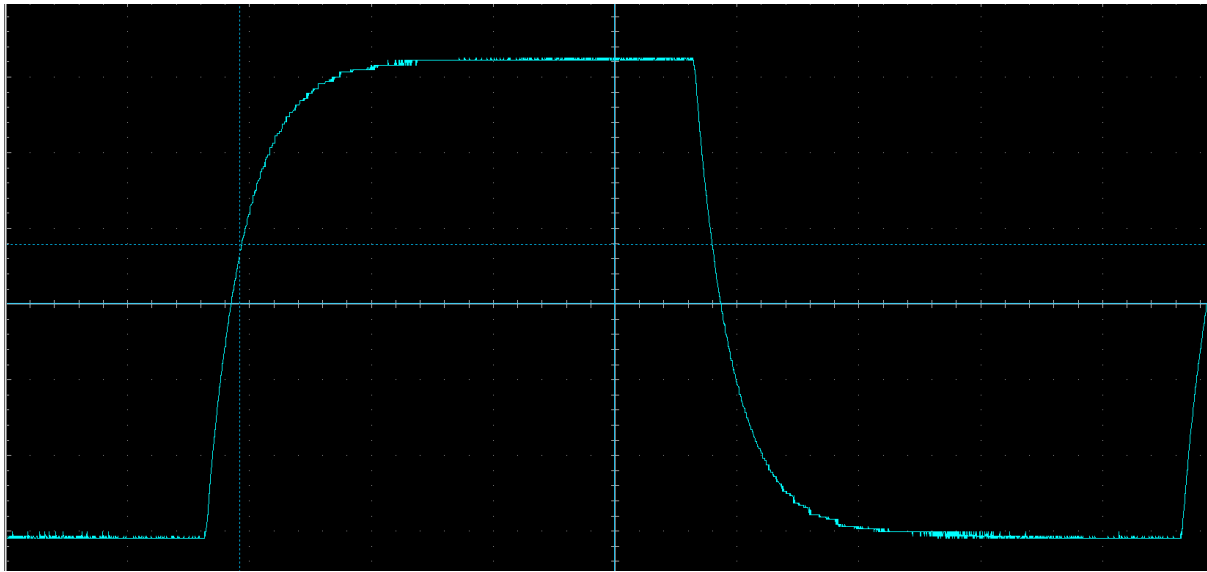


Figure 2 - Capacitor wave marked at 66% charge

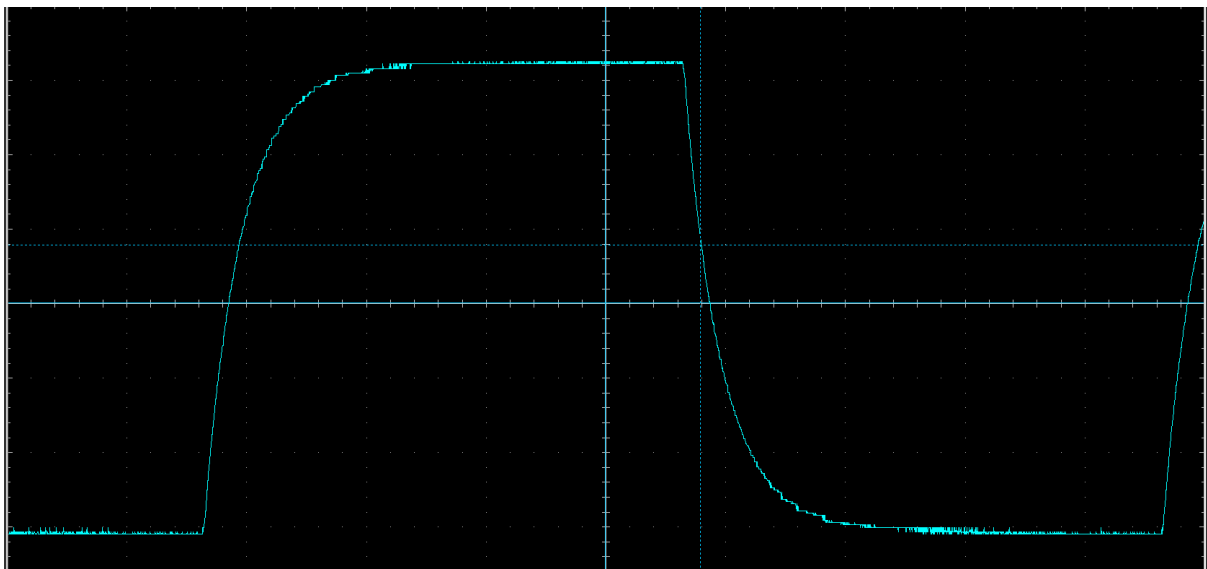


Figure 3- Capacitor wave marked at 33% discharge

1.4 Basic Capacitor Calculations (6)

For the purpose of calculating capacitance in an RC circuit, the following formula may be used. Remembering that Capacitance is measured in Farads. The two equations are both used to find a “time constant” using capacitance multiplied by resistance.

$$\tau = R \times C$$

In the experiment conducted, a 100 ohm resistor was used and a capacitor of 1 μF capacitance was placed into the circuit. Therefore: $100 \times 1 \times 10^{-6} = 100 \times 10^{-4} \text{ S}$ or 100 μs

1.5 Capacitor discharge table (5)

Table 1 – 10 selected data points

		index							
	end	start	Range	"/9"	v	min	V treated	Time (s)	
1	3300	3000	300	33	0.5145	-0.4455	0.96	0.002994	
2		3033			0.2886		0.7341	0.003027	
3		3066			0.1129		0.5584	0.00306	
4		3099			-0.0251		0.4204	0.003093	
5		3132			-0.1443		0.3012	0.003126	
6		3165			-0.2196		0.2259	0.003159	
7		3198			-0.3012		0.1443	0.003192	
8		3231			-0.3576		0.0879	0.003225	
9		3264			-0.4078		0.0377	0.003258	
10		3297			-0.4455		0	0.003291	

Table 2- Capacitor Discharge Table

Time (s)	Voltage (V)	ln (V)	$dy = y_2 - y_1$ $dy = \ln(V)_2 - \ln(V)_1$	$dx = x_2 - x_1$ $dx = \text{Time}_2 - \text{Time}_1$	dy/dx
0.002994	0.96	-0.04082199	x	x	x
0.003027	0.7341	-0.30911002	-0.26829	0.000033	-8129.94016
0.00306	0.5584	-0.58267973	-0.27357	0.000033	-8289.99114
0.003093	0.4204	-0.86654864	-0.28387	0.000033	-8602.08826
0.003126	0.3012	-1.19998078	-0.33343	0.000033	-10104.0043
0.003159	0.2259	-1.48766286	-0.28768	0.000033	-8717.63856
0.003192	0.1443	-1.93586081	-0.4482	0.000033	-13581.7563
0.003225	0.0879	-2.43155547	-0.49569	0.000033	-15021.0503
0.003258	0.0377	-3.27809518	-0.84654	0.000033	-25652.7185
0.003291	0	N/A	N/A	3.3E-05	N/A

1.6 Plot log(V) Gradient (5)

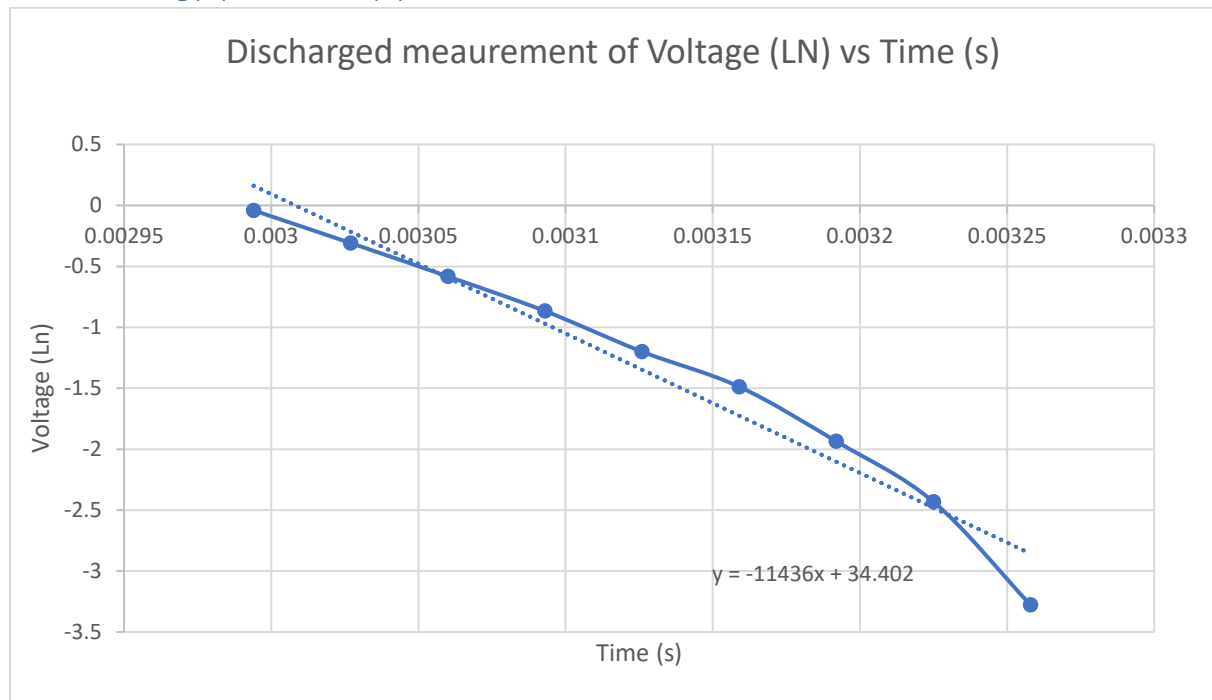


Figure 4 - Natural Log of Voltage plotted against time from excel calculations

1.7 Gradient Calculations and Compare (8)

1.7.1 Gradient Calculations

$$C = \tau/R$$

$$\tau = -1/RC$$

1.7.2 Comparison table

Table 3 - Comparison of expected results with recorded results

	Capacitance	Delta	Percentage difference
Actual	1 μF	x	X
Marker Calculation	81 μF	+ 80 μF	195.122%
Gradient Calculation	87 μF	+ 86 μF	195.455%

1.8 Capacitor Uses (5)

In the automotive industry, capacitors have many uses. To give one in-depth example of how capacitors are used, is their presence within the SW20 MR2 headlight control unit.

One complaint that owners have is to do with the headlight 'pop up time'. Essentially, when flashing the headlights at other drivers, or turning the headlights off, there is a delay before the headlights retract into the closed position. There is a 'fix' to this that involves removing 2 capacitors from the control unit, bridging the circuit where capacitor C2 used to be, and replacing the 47 μF capacitor (C1) with a lower value, 10 μF 16v capacitor. This modification means that the headlight units shut

instantly after the lights stop receiving power. This works because the capacitor within the control unit, that dictates the signals going to the headlight motors, has much shorter discharge time than its unmodified counterpart. See figure 1 for capacitor C1 and C2 on the circuit board.

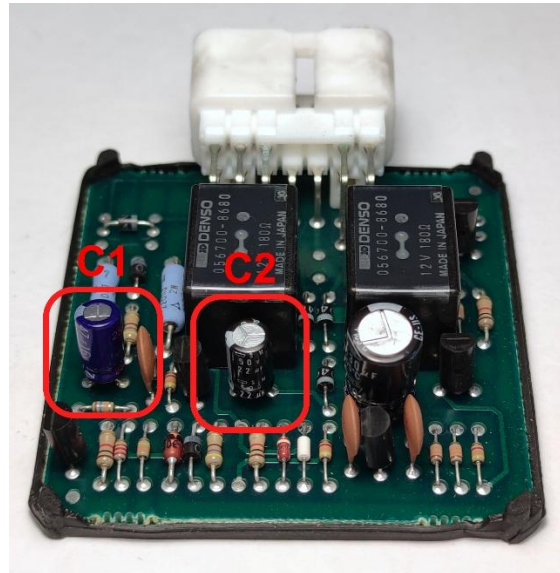


Figure 5 - MR2 SW20 Headlight Control unit Circuit, Highlighting the capacitors being modified (Hrouda, 2023)

Other examples include:

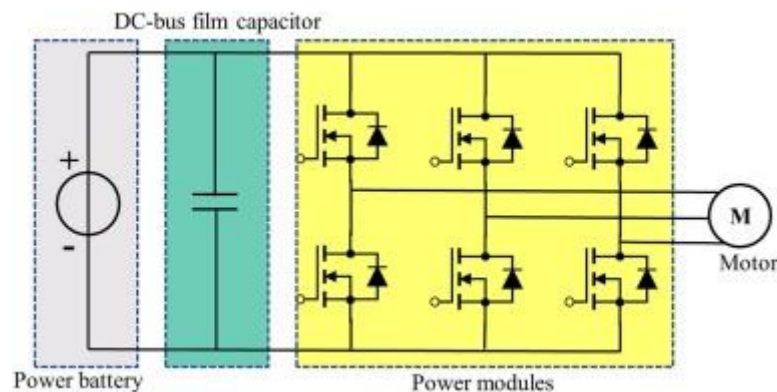


Figure 6 - Capacitor Stabilising Incoming Voltage (Huang et al., 2024)

- Figure 6 shows a capacitor placed between a power battery and different components within a vehicle's power module. In this instance, its purpose is to filter and smooth incoming currents, thus stabilising the voltage delivered to the circuit. (Huang et al., 2024)
- Regenerative Braking systems: Supercapacitors efficiently store quick bursts of energy during braking, reducing stress on the main battery by feeding the power steadily once the brake cycle is complete.
- Power Supply Smoothing: Aluminium filter out alternating current (AC) noise from the alternator, ensuring smooth DC power to sensitive electronic systems.

- Taco Moto sells a capacitor that acts as 'a failsafe for modern KTM/Husqvarna enduro bikes' allowing the bikes to start with a battery that has a charge lower than the minimum voltage required by the systems, by storing some energy in this capacitor.
- High-Performance Audio Systems: Large "stiffening" capacitors act as energy reservoirs. They supply instant power during deep bass hits, preventing headlights from dimming and protecting sensitive electronics from voltage drops.
- Surge Suppression (Snubbers): Industrial switches and relays generate massive voltage spikes when opened. "Snubber" capacitors absorb these spikes to prevent electrical arcing, which would otherwise weld contacts together or damage sensitive semiconductors.
- Energy Storage & Backup (UPS): Capacitors can provide bridge power during brief outages or while switching between power sources, preventing data loss in industrial controllers.
- Start Capacitors: Provide a massive initial burst of energy to help single-phase motors (like those in HVAC units and compressors) overcome inertia.
- Run Capacitors: Maintain a consistent phase shift while the motor is running to ensure smooth operation and efficiency.

1.9 Inaccuracies Question (4)

Many factors can affect the inaccuracy within the data. For example, cheap equipment may induce an unwanted resistance into the circuit, thus giving an incorrect reading, and human error may lead to bad results.

The user manual (Hantek, 2021) states that the device must be recalibrated whenever the ambient room temperature changes by 5°C or more, the testing was being completed in a computer room, during winter, with 30 other students present so the temperature will have likely changed by more than 5°C due to aspects like body heat, and computer exhaust temperatures changing the ambient room temperature. The manual also states that the oscilloscope should be allowed to "warm up" for twenty minutes prior to taking readings to give accurate data. This methodology was not followed during testing and could have skewed the results.

These inaccuracies should be investigated by retesting the circuit.

1.10 Risk Question (10)

As modern vehicles become autonomous and digitalised, threats are ubiquitous. To mitigate this, the International Standard of Organisation (ISO) and the Society of Automotive Engineers (SAE) published the ISO/SAE 21434:2021 standard. (Khalil, Gehrmann and Vogel, 2025)

Released in 2021, the standard defines guidelines to ensure vehicles, over their life cycle, are protected against cyber-related threats

Within modern vehicles, CANBUS systems provide driver assist technologies such as automatic braking.

Often these systems can be accessed remotely. According to Atkinson, DPV Transportation (2025), Autonomous vehicles are attractive targets to hackers. As they provide multiple avenues to attack a vehicle from. The main avenues for attackers are Over-The-Air (OTA) Update systems, Wireless Interfaces and sensor and perception systems.

OTA systems are vulnerable if not secured. A hacker may hijack the update channel and push malicious firmware into the control systems. If this were to happen, multiple vehicles may be at risk.

Wireless interfaces are a proven weakness within manufacturers. The most common attack is the keyless entry system. Buckingham Insurance (2025) used data from the office of national statistics CSEW showing that between March 2023 and 2024, 58% of car thefts were committed via attacks that cloned the RF signal produced between a vehicle and its key fob. Additionally, the Home office via GOV.uk (2025) states 60% of car thefts in London were performed using these attacks.

Science Direct (2025) claims the ISO/SAE standard outlines the TARA (Threat Analysis and Risk Assessment) method to address risk early in the development process.

This method includes identifying critical assets, determining threat and attack vectors, assigning levels of risk, defining mitigation measures and documenting all activities.

While CANBUS are designed to promote efficiency, they carry inherent weaknesses.

CANBUS messages are sent as plain text, with no encryption or authentication. This means that attackers can send spoofed signals without having to pass authentication checks.

While the industry has become aware of cyber-threats, implementing changes presents a challenge. One method to make systems more secure is to add authentication or channel encryption into CAN protocol. However, this introduces issues with backwards compatibility. An additional concern is the payload of CAN networks. Adding this level of encryption would increase the work needed to process each CANBUS signal individually. The issue here is that the network must remain under 50% of its maximum in order to efficiently process and transfer critical messages in real time (Yang, Duan and Tehranipoor, 2020)

2 References

- Atkinson, C. (2025). *Cybersecurity in Autonomous Vehicles: Defending Cars from Hackers*. [online] DPV Transportation. Available at: <https://www.dpvtransportation.com/cybersecurity-autonomous-vehicles/> [Accessed 4 Dec. 2025].
- Buckingham Insurance and Buckingham Insurance (2025). *Keyless Car Theft Surge: Is Your Vehicle at Risk and What Can You Do about It? - General Insurance Brokers UK | Buckingham Insurance*. [online] General Insurance Brokers UK | Buckingham Insurance. Available at: <https://buckinghaminsurance.co.uk/keyless-car-theft-surge-is-your-vehicle-at-risk-and-what-can-you-do-about-it/> [Accessed 19 Apr. 2026].
- CSS Electronics (2021). *CAN Bus Explained - A Simple Intro [v2.0 | 2021]* 🌟. [online] YouTube. Available at: <https://www.youtube.com/watch?v=oYps7vT708E> [Accessed 4 Dec. 2025].
- CyberROAD: A cybersecurity risk assessment ontology for automotive domain aligned with ISO/SAE 21434:2021 - ScienceDirect*. (n.d.). Retrieved April 19, 2026, from <https://www.sciencedirect.com.uwtsd.idm.oclc.org/science/article/pii/S2214212625000535>
- Ebrahimi, M., Castella Triginer, J., & Schmittner, C. (2022). Identification and Verification of Attack-Tree Threat Models in Connected Vehicles. *SAE Technical Papers*. <https://doi.org/10.4271/2022-01-7087>
- Fernandez de Arroyabe, I., Watson, T., & Angelopoulou, O. (2023). Cybersecurity in the Automotive Industry: A Systematic Literature Review (SLR). *Journal of Computer Information Systems*, 63(3), 716–734. <https://doi.org/10.1080/08874417.2022.2103853>
- GoTech (2023). *CAN Bus Communication Explained (Part 1)*. [online] YouTube. Available at: <https://www.youtube.com/watch?v=YbF3idCk4EQ> [Accessed 4 Dec. 2025].
- Hantek (2021). *USER'S MANUAL Hantek6022BE*. [online] Available at: https://www.hantek.com/uploadpic/hantek/files/20210609/Hantek6022BE_Manual_EN.pdf [Accessed 19 Apr. 2026].
- Ho, J. S., & Greenbaum, S. G. (2018). Polymer Capacitor Dielectrics for High Temperature Applications. *ACS Applied Materials and Interfaces*, 10(35), 29189–29218. <https://doi.org/10.1021/ACSAMI.8B07705>
- Hrouda, M. (2023). Toyota MR2 Pop-up Headlights Delay Delete Mod. Available at: <https://blog.michalhrouda.cz/2023/02/toyota-mr2-pop-up-headlights-delay-delete-mod/> [Accessed 10 Apr. 2026].
- Huang, L., Yuan, T., Wang, Y., Guo, H., Guo, X., Li, X., Chang, B., Wang, Y. and Xi, X. (2024). Numerical Investigation and Optimization on Thermal Management of a DC-bus Film Capacitor in Electric Vehicle Using Microchannel Cooling Plates. *Applied Thermal Engineering*, [online] 244. doi:<https://doi.org/10.1016/J.APPLTHERMALENG.2024.122695>.

ISO (2021). *ISO/SAE 21434*. [online] ISO. Available at: <https://www.iso.org/standard/70918.html> [Accessed 19 Apr. 2026].

Khalil, K., Gehrmann, C. and Vogel, G. (2025). *CyberROAD: a Cybersecurity Risk Assessment Ontology for Automotive Domain Aligned with ISO/SAE 21434:2021*. [online] Science Direct. Available at: <https://www-sciencedirect-com.uwtsd.idm.oclc.org/science/article/pii/S2214212625000535> [Accessed 17 Apr. 2026].

Office, H. and GOV.UK (2025). *Vehicle Theft Equipment to Be Banned under New Government Law*. [online] GOV.UK. Available at: <https://www.gov.uk/government/news/vehicle-theft-equipment-to-be-banned-under-new-government-law> [Accessed 19 Apr. 2026].

Pan, L., Zheng, X., Chen, H. X., Luan, T., Bootwala, H., & Batten, L. (2017). Cyber security attacks to modern vehicular systems. *Journal of Information Security and Applications*, 36, 90–100. <https://doi.org/10.1016/j.jisa.2017.08.005>

Wu, X., Chen, X., Zhang, Q. M., & Tan, D. Q. (2022). Advanced dielectric polymers for energy storage. *Energy Storage Materials*, 44, 29–47. <https://doi.org/10.1016/j.ensm.2021.10.010>

Yang, Y., Duan, Z. and Tehranipoor, M. (2020). Identify a Spoofing Attack on an In-Vehicle CAN Bus Based on the Deep Features of an ECU Fingerprint Signal. *Smart Cities*, [online] 3(1), pp.17–30. doi:<https://doi.org/10.3390/smartcities3010002>.