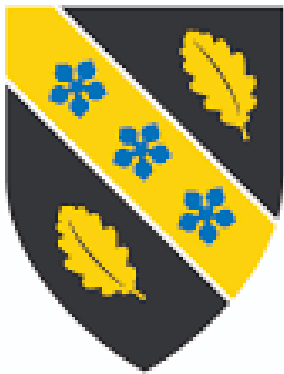


University of Wales Trinity Saint David

Wales Institute of Science & Art



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

ENGINEERING SKILLS TECHNICAL REPORT

Engineering Skills (ACHA4022A)

Rebekah Pratt

2400239

Date (11/2025)

Word Count:

Table of Contents

Table of Abbreviations	i
Table of Figures	ii
1. Introduction.....	1
2. Health and Safety Risk Assessment.....	2
3. Security Risk Matrix	4
3.1 Security Risk 1: Software Malfunction.....	4
3.2 Security Risk 2: Remote Vehicle Hacking	4
3.3 Security Risk 3: Vehicle Theft	4
3.4 Security Risk 4: Ransomware Attack	5
4. Engineers' Role in Society	6
5. Problem Solving.....	7
6. Team Structure	9
7. Conclusion	11
8. References.....	12

Table of Abbreviations

Abbreviations	Meaning
PPE	Personal Protective Equipment
PUWER	Provisions and Use of Work Equipment Regulations 1988
UK	United Kingdom
IMechE	Institution of Mechanical Engineering
HSWA	Health and Safety at Work Act 1974
COSHH	Control of Substances Hazardous to Health
LEV	Local Exhaust Ventilation
SDS	Safety Data Sheets
ECU	Electronic Control Units

Table of Figures

Figure 1: Risk Assessment for Composite Material Work.....	3
Figure 2: Security Risk Matrix diagram	5
Figure 3: Eight Disciplines (8D) Problem Solving (Quality Gurus, n.d.)	7
Figure 4: Hierarchical Athletics Coaching Structure	9
Figure 5: Flat Coaching Structure Diagram.....	10

1. Introduction

This report examines key engineering principles across five areas central to engineering. It begins by evaluating a selected workshop activity through a risk assessment which is supported by relevant health and safety legislation. A security risk matrix is then used to analyse four physical and digital threats and propose appropriate engineering responses. The report also considers an engineer's role in society by comparing two professional codes of conduct with emphasis on sustainability and environmental responsibility. Problem solving methods used in product development are explored through research and supporting flow diagrams. Finally, a personal reflection reviews the effectiveness of a previously experienced team structure and assesses an alternative structure backed by research.

2. Health and Safety Risk Assessment

Health and Safety is a critical aspect of engineering due to the hazardous nature of many workshop-based activities. Working with composite materials, such as carbon fibre and fibreglass, is a good example of this. Processes used in composite work can create dust, involve chemical resins as well as require the use of machinery, all of which present significant risks if not properly controlled.

The Health and Safety at Work etc. Act 1974 (HSWA) places a general duty on the university, as an employer and teaching facility, to ensure the health, safety and welfare of all persons “so far as is reasonably practicable” (HSWA, 1974). In the context of composite work, this means ensuring the workshop environment is safe, providing suitable ventilation, keeping walkways clear of dust and off-cuts, and ensuring that equipment such as extraction systems and hand tools are safely maintained. HSWA also requires the university to provide adequate training, supervision and information. Therefore, students working with composite materials must receive appropriate training in safe sanding methods, correct PPE usage and chemical-handling procedures.

The Control of Substances Hazardous to Health Regulations 2002 (COSHH) are particularly important because composite work produces hazardous airborne dust and involves chemicals such as epoxy resins, catalysts and solvents. COSHH requires a written risk assessment, identification of exposure routes, and implementation of systems to control harmful substances (COSHH, 2002). In the workshop, this includes using Local Exhaust Ventilation (LEV), using wet-sanding techniques to reduce dust, providing respirators suitable for fine particles, and ensuring that Safety Data Sheets (SDS) are available for all resins and hardeners. As epoxy resins can cause skin sensitisation, COSHH also justifies the requirement for gloves, protective clothing and good hygiene practices.

The Provision and Use of Work Equipment Regulations 1998 (PUWER) apply to machinery commonly used in composite workshops, including band saws, grinders, sanders and extraction units. PUWER requires equipment to be suitably maintained and used only by trained and competent persons (PUWER, 1998). This supports the need for pre-use checks, machine guarding, emergency-stop systems, and supervision for inexperienced users. PUWER also requires that equipment be inspected and recorded, ensuring tools used on composites remain safe and capable of handling fibre-reinforced materials without excessive vibration or kickback.

Finally, composite waste such as resin-contaminated cloth, fibre off-cuts and dust must be disposed of safely under environmental waste-management regulations. The university is therefore responsible for providing sealed, labelled waste bins and ensuring that hazardous waste collections are correctly arranged.

Together, HSWA, COSHH and PUWER provide a comprehensive legal basis for managing risks associated with composite-material work and ensuring that exposure to chemical, mechanical and airborne hazards is effectively controlled.

Risk Assessment: Composite Material Work								
Hazard	Potential Harm	Persons at Risk	Existing / Required Control Measures	PPE Required	Likelihood (L)	Severity (S)	Risk Rating (LxS)	Person Responsible
Airborne dust & fibres from sanding/cutting carbon-fibre or fibreglass	- Respiratory irritation - eye irritation - skin rash	- Students - Technicians - Workshop users - Cleaners	- Local Exhaust Ventilation (LEV) - Dust extraction - Wet cutting/sanding method - Clean-up procedures - Signage	- Dust mask - Safety goggles - Long-sleeve clothes - Gloves	4	4	16 (High)	Workshop Supervisor / User
Resins, hardeners & solvents	- Chemical burns, - allergic skin response - respiratory irritation	- Students - Technicians - Workshop users - Waste handlers	- COSHH assessment - Use SDS - Nitrile gloves - Good ventilation - Spill kits - No food/drink	- Nitrile gloves - Goggles - Dust Mask	3	4	12 (Medium)	Workshop Manager / Lab Technician
Waste dust or resin build-up	- Fire hazard, - explosion risk - environmental contamination - cross-contamination	All workshop users	- Frequent housekeeping - Sealed waste containers, - Correct disposal, - Anti-static cleaning equipment	- Dust mask - Safety gloves	3	5	15 (High)	Workshop Supervisor
Tools / machinery (grinders, saws, sanders)	- Cuts - abrasions, - entanglement - noise-induced hearing loss	- Students - Technicians	- Training & authorisation only - Machine guards - Emergency stops, - Hearing protection - Secure clamping	- Dust mask - Safety gloves - Hearing Protection	3	4	12 (Medium)	Trainer / Competent User
Slip / trip hazard from dust, offcuts or spillages	- Sprains - Fractures - Falls	All workshop users	- Housekeeping - Clear walkways - Prompt spill clean-up - Floors kept dry	- Safety gloves - Steel-toe footwear	2	3	6 (Low)	Workshop Supervisor
Incorrect handling / storage of materials	- Injury from heavy components - Damage to chemicals	- Students - Technicians	- Manual handling training - Labelled chemical storage - Shelving	- Safety gloves - Steel-toe footwear	2	3	6 (Low)	Workshop Supervisor

Figure 1: Risk Assessment for Composite Material Work

3. Security Risk Matrix

3.1 Security Risk 1: Software Malfunction

A software malfunction can pose a significant security risk even if it isn't caused by a cyberattack. Crashes and glitches can expose sensitive data, disable protection software and leave systems vulnerable to exploitation. An example of this is the CrowdStrike software malfunction in 2024, which impacted Mercedes Formula One team during the first practice session of the Hungarian Grand Prix (Sky Sports, 2024). Although only the pit wall was largely affected by the IT outage, the disruption hindered engineers' ability to access real-time telemetry and strategy data, demonstrating how small software failures can interfere with smooth running operations.. While no data was stolen, the incident highlights that even brief malfunctions can expose teams to operational risks and potential security threats, emphasising the need for tough contingency measures in high-stake, technology dependent environments.

3.2 Security Risk 2: Remote Vehicle Hacking

Modern vehicles are essentially computers on wheels, with numerous electronic control units (ECU) managing everything from steering and braking to entertainment systems. Hackers can exploit any vulnerabilities to gain control over critical functions, steal personal data or facilitate theft. The increased integration of over-the-air updates, Wi-Fi connectivity and cloud-synchronised infotainment systems expands the vehicle's attack surface. Vulnerabilities in gateway ECUs or telematics modules allow an attacker to pivot into critical subsystems such as braking or steering, significantly elevating the impact score. (Checkoway et al., n.d.). An example of a vehicle that is easily susceptible to remote vehicle hacking is Jeeps. The vulnerability was demonstrated in 2015 when security researchers remotely compromised a Jeep Cherokee through its Uconnect infotainment system. By exploiting vulnerabilities in the cellular-connected head unit, they accessed the vehicles internal systems and were able to manipulate critical functions such as brakes, transmissions and steering from miles away (WIRED, 2015).

3.3 Security Risk 3: Vehicle Theft

Vehicle theft remains a significant physical security risk for the automotive industry and BMW models have often been targeted due to their high value and adoption of keyless entry systems. Thieves commonly use relay attacks, where they amplify the signal of keyless entry systems from a key fob inside a home to unlock and start the vehicle within seconds. BMW were found to have 14 different flaws, according to a study by a Chinese cyber-security lab (BBC News, 2018).

3.4 Security Risk 4: Ransomware Attack

In February 2022, Toyota experienced a major operational disruption when its key supplier, Kojima Industries, was hit by a suspected ransomware attack. The supplier discovered a virus and a threatening message on its servers, forcing it to shut down its systems and halt communication with Toyota. As Kojima provides essential plastic and electronic components, Toyota was compelled to suspend production across all 14 of its factories in Japan, stopping 28 production lines. This single-day shutdown delayed the manufacture of approximately 13,000 vehicles. The incident highlighted the automotive industry's vulnerability to supply-chain cyberattacks and demonstrated how digital breaches can directly impact large-scale manufacturing.

Likelihood+ / Impact→	1-Insignificant	2-Minor	3-Moderate	4-Major	5-Critical
1-Rare	Low	Low	Low	Medium	High
2-Unlikely	Low	Low	Medium	Medium	High
3-Possible	Low	Software Malfunction (6)	Medium	High	Remote Vehicle Hacking (15)
4-Likely	Medium	Medium	High	Vehicle Theft (16)	Ransomware Attack (20)
5-Almost Certain	Medium	Medium	High	Extreme	Extreme
	Risk Rating	1-5 (Low)	5-9 (Medium)	10-14 (High)	15-25 (Extreme)

Figure 2: Security Risk Matrix diagram

Based on the risk matrix, ransomware receives the highest risk score of 20 due to its combination of high likelihood and severe safety consequences. Due to its high risk, ransomware attacks require a layered, defence approach that protects both technical systems and organisational processes. Key measures include implementing critical manufacturing and administrative networks to limit the spread of malware, as well as the use of multi-factor authentication to secure high-privilege accounts (Office H, 2024). In addition, the automotive sector can strengthen supplier and third-party security through audits and shared cyber-security standards, as supply chain breaches have proven highly disruptive (UK Government, 2025).

4. Engineers' Role in Society

Chartered Engineers are expected to maintain high ethical and professional standards, guided by established codes of conduct. In the UK, this is upheld by two organisations that publish these ethical frameworks are the Engineering Council and the Institution of Mechanical Engineering (IMechE).

The Engineering Council establishes the primary ethical framework for all UK-registered engineers through its Guidance on Ethical Principles (Engc.org.uk, 2017). This document outlines four fundamental principles: honesty and integrity, respect for life, law, the environment, and the public good, accuracy and rigour, and leadership and communication. These principles form the foundation of professional behaviour and ensure that engineers act responsibly in protecting public welfare and the environment. The principle of 'respect for life, law and the environment' is particularly relevant to the automotive and motorsport industry.

In motorsport, the principle of "respect for life and the environment" is vital, requiring engineers to consider emissions, material waste, energy efficiency, and the integration of sustainable technologies when designing and improving race cars.

The IMechE code of conduct (Institution of Mechanical Engineers, 2023) complements the Engineering Council's framework by translating these values into specific expectations for mechanical and automotive engineers. It emphasises competence, integrity, and responsibility to the public, requiring engineers to ensure their work supports safety and minimises environmental harm. Within motorsport, this extends to developing more efficient power units, promoting sustainable fuels, and implementing recycling or energy-recovery systems to reduce carbon impact.

Both organisations highlight that an engineer's role extends beyond technical problem-solving to include environmental and societal responsibilities. By integrating sustainability into engineering design practices, for example, hybrid systems and lightweight materials, allows engineers to contribute to reducing environmental impact while advancing performance. Following these ethical codes ensures that engineers in motorsport and the automotive sector perform to a professional standard while also supporting both technological advancements as well as global sustainability goals.

5. Problem Solving

Within Motorsport teams, problems are an inevitable part of developing high performance vehicles, whether during design, testing or race preparation. These issues can range from electronic malfunctions, aerodynamic inefficiencies or mechanical failures. Teams approach problem solving through highly structured methods such as Eight Discipline (8D) problem solving, Root Cause Analysis and Ishikawa diagram. 8D analysis is a structured problem-solving method used to identify the root cause of defects and to implement corrective and preventive actions. (MDPI, 2023).

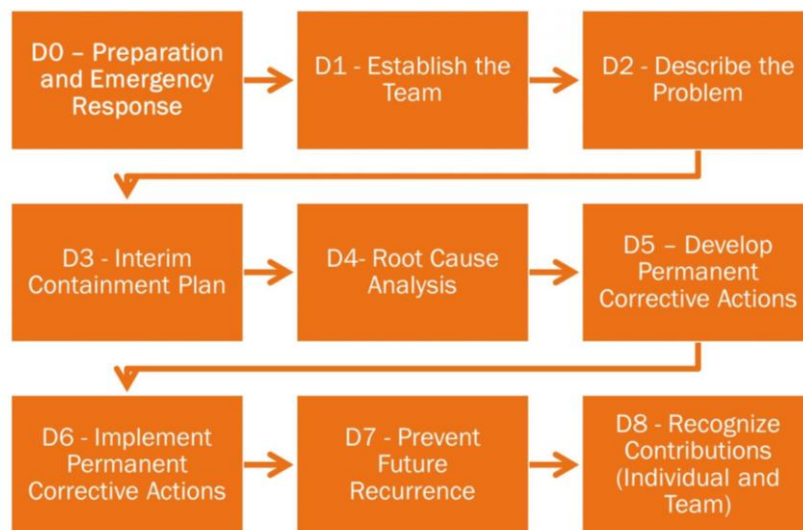


Figure 3: Eight Disciplines (8D) Problem Solving (Quality Gurus, n.d.)

Figure 3 shows the full 8D problem-solving process, beginning with D0, where the team prepares and puts immediate emergency measures in place to manage the issue. D1 involves establishing a team, followed by D2, where the problem is clearly described and defined. In D3, an interim containment plan is created to control the issue temporarily while investigation continues. D4 focuses on root-cause analysis to identify the true underlying cause of the problem, leading to D5, where permanent corrective actions are developed. These actions are then carried out and validated in D6, ensuring they effectively resolve the issue. D7 aims to prevent future recurrence by updating processes, documentation, and training, and the process concludes with D8, which recognises the contributions of the individuals and the team involved in solving the problem (Quality Gurus, n.d.).

The 8D model helps engineering teams by providing a structured method to identify, analyse and fix issues found during development. It ensures problems are clearly defined, root causes are identified and effective long-term solutions are implemented. By involving a cross-functional team and using interim containment, it prevents further impact while investigation continues. The process also

improves future work by updating procedures to stop the issue recurring, strengthening reliability and overall project quality.

6. Team Structure

During my time as an Assistant Coach at Swansea Harriers Athletics Club, I worked as part of a coaching team of six people supporting young athletes aged 9–13 across sprints, endurance, jumps and throws. My role involves assisting the lead coaches with session planning, delivering drills, monitoring technique, encouraging participation, and ensuring a safe, engaging environment for the children. This also required coordination with other coaches to manage session timing, warm-ups, equipment, and athlete progression across multiple disciplines.

The team works in a hierarchical structure with the head coach holding overall responsibility for the session, while the lead coaches for each discipline direct their respective sessions and assistant coaches like myself follow their guidance.

The hierarchical structure has several advantages. It provides clear lines of authority and accountability, making it easy to know who to report to and who made final decisions about training, safety, and progression. Within each session, responsibilities are clearly defined, which helps to maintain structure and organisation. Communication is generally straightforward, as instructions flow from top-down from the Head Coach to lead coaches, and then to assistants. This ensures consistency in session delivery and adherence to club policies.

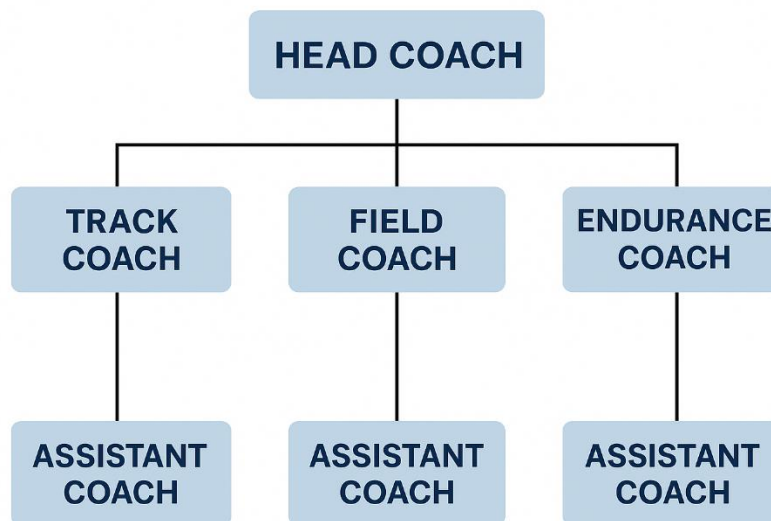


Figure 4: Hierarchical Athletics Coaching Structure

However, the hierarchical structure also has limitations. Decision making is concentrated at the top, assistant coaches have limited freedom to adjust sessions or respond immediately to individual athlete needs. Coordination between different discipline groups is less flexible, so athletes participating in multiple events sometimes experience conflicting guidance. Additionally, information about athlete

progression or issues often required reporting up the chain before solutions could be implemented, which sometimes delayed adjustments to training plans. Although this is not necessary at this level due to it only being a development group, this can still impact athletes at later times.

An alternative to the hierarchical structure is the flat structure. Flat team structure in athletics coaching emphasises collaboration and shared responsibility by minimising hierarchy. Instead of a traditional top-down approach, where a head coach dictates all decisions, coaches and even athletes contribute to training strategies, competition planning, and athlete development. This approach uses open communication and empowers athletes to take ownership of their progress, while allowing staff to share expertise across disciplines such as strength, conditioning, and mental performance. Although it can increase engagement and adaptability, flat structures require high competence, clear communication, and effective conflict management to prevent role confusion or decision delays.

This approach would ideally work better with older athletes however an adapted version could be used for the age range that I coach.

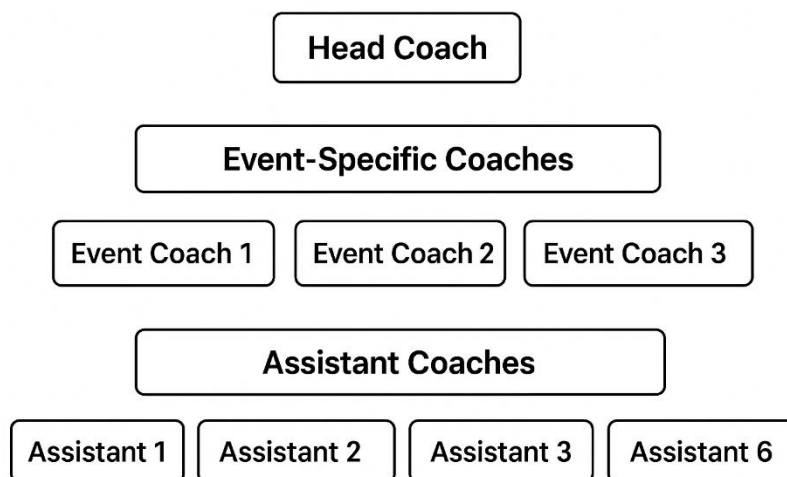


Figure 5: Flat Coaching Structure Diagram

7. Conclusion

In conclusion, this report shows that safe engineering work depends on following the right laws, using good problem-solving methods and acting responsibly as an engineer. Rules like HSWA, COSHH and PUWER help keep university workshops safe by reducing risks from dust, chemicals and machinery. The security-risk section shows that modern engineering systems can be affected by software failures, hacking and other threats, so strong protections are needed. Ethical guidelines from the Engineering Council and IMechE remind engineers to work safely, honestly and with care for the environment. Methods like the 8D model and clear team structures help engineers solve problems properly and work well together. Overall, engineering is not just about technical skills, it also requires safety, teamwork and responsibility.

8. References

BMW cars found to contain more than a dozen flaws (2018) *BBC News* [online], 23 May. Available at: <https://www.bbc.co.uk/news/technology-44224794> [Accessed: 3 December 2025].

Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H., Savage, S., Koscher, K., Czeskis, A., Roesner, F. and Kohno, T. (n.d.). *Comprehensive Experimental Analyses of Automotive Attack Surfaces*. [online] Available at: https://www.usenix.org/legacy/events/sec11/tech/full_papers/Checkoway.pdf

Cirtina, L.-M., Dumitrascu, A.-E., Cazacu, D.V., Ianasi, C.A., Rădulescu, C., Tătar, A.M., Pasăre, M.M., Nioață, A. and Cirtina, D. (2025) ‘Eight-disciplines analysis method and quality planning for optimising problem-solving in the automotive sector: A case study’, *Processes* [online], 13(10), p. 3121. Available at: <https://www.mdpi.com/2227-9717/13/10/3121> [Accessed: 5 December 2025].

Eight Disciplines (8D) Problem Solving (no date) *Quality Gurus* [online]. Available at: <https://qualitygurus.com/eight-disciplines-8d-problem-solving/> [Accessed: 3 December 2025].

Engc.org.uk (2017) *Guidance on ethical practices* [online]. Available at: : <https://www.engc.org.uk/standards-guidance/guidance/guidance-on-ethical-principles/> [Accessed: 17 November 2025].

Health and Safety Executive (2024) *Health and Safety at Work etc. Act 1974* [online]. Available at: <https://www.hse.gov.uk/legislation/hswa.htm> [Accessed: 17 November 2025].

Help Net Security (2018) *Researchers hack BMW cars, discover 14 vulnerabilities* [online]. Available at: <https://www.helpnetsecurity.com/2018/05/23/bmw-vulnerabilities/> [Accessed: 20 November 2025].

Institution of Mechanical Engineers (2023) *Code of Conduct explained* [online]. Available at: <https://www.imeche.org/membership-registration/become-a-member/code-of-conduct> [Accessed: 20 November 2025].

Leggett, T. (2025) ‘Jaguar Land Rover posts heavy loss after cyber-attack’, *BBC News* [online], 14 November. Available at: <https://www.bbc.co.uk/news/business-67369165> [Accessed: 1 December 2025].

Office for Health (2024) *CRI guidance for organisations during ransomware incidents* [online]. Available at: <https://www.gov.uk/government/publications/cri-guidance-for-organisations-during-ransomware-incidents> [Accessed: 4 December 2025].

Office for Health (2025) *Guidance for organisations to build supply chain resilience against ransomware* [online]. Available at: <https://www.gov.uk/government/publications/supply-chain-resilience-against->

[ransomware/guidance-for-organisations-to-build-supply-chain-resilience-against-ransomware](#) [Accessed: 2 December 2025].

Sky Sports (2024) *Global IT outage impacts Mercedes F1 team's pit wall screens at Hungarian GP* [online]. Available at: <https://www.skysports.com/f1/news/12433/13180880/global-it-outage-impacts-mercedes-f1-teams-pit-wall-screens-at-hungarian-gp> [Accessed: 20 November 2025].

Solon, O. (2016) 'Team of hackers take remote control of Tesla Model S from 12 miles away', *The Guardian* [online], 20 September. Available at: <https://www.theguardian.com/technology/2016/sep/20/tesla-model-s-chinese-hack-remote-control-brakes> [Accessed: 25 November 2025].

Toyota to close Japanese factories after suspected cyber-attack (2022) *BBC News* [online], 28 February. Available at: <https://www.bbc.co.uk/news/technology-60521983> [Accessed: 2 December 2025].

WIRED (2015) *Hackers remotely kill a Jeep on a highway* [online video]. YouTube. Available at: <https://www.youtube.com/watch?v=MK0SrxBC1xs> [Accessed: 2 December 2025].