

University of Wales Trinity St David

(UWTSD)

Institute of Science & Art



Engineering Skills Technical Report

Engineering Skills ACHA4022A

Name: Harry Glynn

Student Number: 2505630

Date of Report: 12/2025

Contents

1	Introduction.....	3
2	Health & Safety with Risk Assessments	4
3	Security Risk Matrix	5
3.1	Risk Matrix	5
3.1.1	Vulnerabilities associated with electric vehicles.	6
4	Engineers Role in Society.....	8
5	Problem Solving.....	10
5.1	Lean Problem Solving	10
5.1.1	Plan-Do-Check-Act (PDCA) Method	11
6	Team Structure	12
7	Conclusion.....	13

Tables and Figures

Table 1 - Example Risk Matrix	5
Figure 1 Risk Matrix from HSE.....	5
Figure 2 - Lean Fishbone Diagram (Lean Six Sigma Definition, 2020).....	10
Figure 3 - Plan, Do, Check, Act (Plan, do, check, act – the PDCA cycle — BiteSize Learning, 2025)	11

1 Introduction

This report gives an overview of engineering in three main areas: health and safety (including risk assessments and matrices), the role engineers play in society and how their services improve lives, and how problem solving and teamwork, with different points of view, can significantly benefit engineering projects.

2 Health & Safety with Risk Assessments

Health and safety are a considerably large part of engineering, especially when machinery such as lathes are involved. At the University, a student may be required to operate a lathe in the workshop to shape components. Before this can be done safely, a risk assessment must be carried out to discover what dangers could be present and what injuries could occur to the person performing the task. Law dictates that securing the health, safety and welfare of persons at work must be followed and entertained within any place of work (Parliament, HSW Act, 1974). The Health and Safety at Work etc. Act 1974 is supported by the Management of Health and Safety at Work Regulations 1999, which require suitable and sufficient risk assessments, health surveillance where needed and adequate training so that employees remain competent and safe (Parliament, The Management of Health and Safety at Work Regulations 1999, 1999).

For lathe work, other regulations are also relevant. The Provision and Use of Work Equipment Regulations (PUWER) require that the lathe is suitable for use, maintained in a safe condition and that users are trained and supervised (Parliament, The Management of Health and Safety at Work Regulations 1999, 1999). The Personal Protective Equipment at Work Regulations make sure that PPE such as eye protection and safety footwear is provided and used where risks cannot be controlled by other means (Parliament, 1992). Where work with fluids or chemicals are used, the Control of Substances Hazardous to Health Regulations (COSHH) also apply (Parliament, 2002).

A simple risk assessment for using the lathe would look at hazards such as getting tangled in rotating parts, flying swarf, sharp edges and noise. Entanglement with the rotating chuck or workpiece would be classed as a high-severity hazard with a medium likelihood, giving a high initial risk level. A way to prevent this would include tying back long hair, removing jewellery, avoiding loose clothing and ensuring guards are in place, which would reduce the risk to low. Flying swarf and chips present a medium risk of eye injury, which can be minimised by wearing safety goggles and keeping the work area tidy. The required PPE for this task would typically be safety goggles, a dust coat or overalls, steel-toed boots and possibly hearing protection. An in-depth risk assessment would consider all these factors plus training to make sure that the student and others remain safe around the machine.

3 Security Risk Matrix

Risk Matrix

Table 1 - Example Risk Matrix

	Minor	Moderate	Severe
Very likely	Medium	Medium - High	High
Likely	Low - Medium	Medium	Medium - High
Unlikely	Low	Low - Medium	Medium

A risk matrix takes possible issues; how likely they are to happen and then the impact it would have, should it happen, into account and then gives a risk evaluation based on such. This report will look at some risks associated with autonomous and self-driving electrical vehicles.

Risk Based Approach - Risk Model (Initial Decision Matrix)

Possible injury risk/ possible health risk	Number of possible casualties at one time				
Serious Personal Injury (fatal or major) or Serious Health Effect (permanent, progressive or irreversible condition, or permanently disabling)	Multiple	Red	Red	Red	Amber
	Single or low	Red	Red	Amber	Amber
Significant Injury (RIDDOR reportable) or Significant Health Effect (non-permanent, reversible or non-progressive condition, or temporary disability)	Multiple	Red	Amber	Amber	Green
	Single or low	Amber	Amber	Green	Green
Minor Injury (non-RIDDOR, first-aid only) or Minor Health Effect (conditions not included above)	Multiple	Amber	Green	Green	Green
	Single or low	Green	Green	Green	Green
	Likelihood	Probable	Possible	Remote	Nil/negligible

Colour key
 Red = follow up complaint as a priority
 Amber = follow up complaint
 Green = do not follow up complaint

Figure 1 Risk Matrix from HSE

3.1.1 Vulnerabilities associated with electric vehicles.

As modern electric and autonomous vehicles become more connected, they are exposed to both digital and physical security threats. A risk matrix can be used to evaluate these threats by considering how likely they are to occur and the impact they would have if they did. This section looks at four realistic threats related to electric vehicles and their charging infrastructure.

The first threat is a cyberattacks that disables large numbers of EV charging stations or disrupts their operation. Recent reports show rising attacks on EV charging networks, with incidents that can shut down chargers and disrupt service to many users (Automotive News, 2025). Such an attack is likely, and while it mainly causes disruption rather than direct physical harm, the impact on users and service providers is moderate, so this is rated as Likely and Moderate, giving it a medium risk.

The second threat is data manipulation within EV charging networks, where attackers alter charging or billing data. Research has shown that cyberattacks on EV charging infrastructure can manipulate charging power and timing, threatening grid stability and potentially leading to financial losses and damaged equipment (Jacob et al., 2025). This type of attack is likely and could have severe consequences for both the power grid and vehicles, so it is rated as Likely and Severe, giving a Medium–High to High risk.

A third, more physical threat is keyless vehicle theft using relay attacks. Attackers capture and relay the signal from a vehicle's key fob to unlock and start the vehicle without physical access to the key. This has been widely reported as a growing method of vehicle theft, making it very likely, but its impact is mainly financial loss and loss of the vehicle rather than wider system damage, so it can be assessed as Very Likely and Moderate, giving a Medium–High risk (Automotive News, 2025).

A fourth threat is physical tampering with charging cables or hardware, such as cutting cables, damaging connectors or installing malicious devices on public chargers. This kind of vandalism or tampering is possible but less frequent and normally localised, so it is considered Unlikely with a Moderate impact, giving a Low–Medium risk (Upstream Security, 2024).

From this analysis, the highest risk is the cyberattack that manipulates charging data and behaviour across EV charging networks, because it is likely to occur and can have a severe impact on both the power grid and the vehicles connected to it (Jacob et al., 2025). A holistic and proportional engineering response would combine secure communication protocols (for example enforcing strong encryption and authentication on charger-to-backend links), continuous anomaly detection at both charger and grid level using data-driven models to spot unusual charging patterns, and proper network segmentation so that a compromised charger cannot easily spread an attack across the whole system (Jacob et al., 2025; Upstream Security, 2024). This should be supported by regular security testing, software update processes and clear incident response plans across vehicle manufacturers, charge point operators and grid operators to reduce the likelihood and impact of such attacks (Upstream Security, 2024).

4 Engineers Role in Society

Being a chartered engineer means that they are held to a high standard within their area of expertise and have reached a professional level through a tested process. There are many organisations which help engineers become chartered engineers such as: the National Society of Professional Engineers (NSPE), Institution of Civil Engineers (ICE), Institution of Engineering and Technology (IET), and Chartered Institution of Building Services Engineers (CIBSE), etc.

All the organisations publish codes of conducts that must be followed for an engineer to become a chartered engineer, these all tend to follow a similar line of conduct and ethics. For example, the IET's code of conduct goes along the lines that all engineer's should exercise their professional skill and judgment as best they can and that they should continue with any professional developments revolving around their chosen specialty to the boards established or set standard (Institution of Engineering and Technology, 2024). These by-laws share similarities throughout the organisations as can be seen with the NSPE which shares a similar code of conduct to the IET; ensuring that all work is their own and that other engineers will not falsely be discredited and that engineers shall acknowledge their own errors and mistakes (National Society of Professional Engineers, 2019). Both organisations have the same basic principles but the IET focuses more on the advancement of technology and innovation whereas the NSPE has more of an outlook on the engineers impact with the public and their relations.

Both organisations look at environmental damage and how best to prevent it both mentioning it in unique ways; in the IET code of conduct it is mentioned that damage to the environment and any breach of legal obligations will not be tolerated and will be dealt with accordingly (Institution of Engineering and Technology, 2024). In the NSPE code of conduct however, it flows around the public and the impact that engineers can have on the environment and in turn the public (National Society of Professional Engineers, 2019). For a motor vehicle engineer this means that responsibility does not stop at making a vehicle fast or reliable; they must also consider fuel consumption, exhaust emissions, noise and how the

vehicle will be disposed of or recycled at the end of its life. Meeting these codes of conduct would therefore require an automotive engineer to design vehicles that meet or exceed environmental regulations, to minimise harmful emissions and waste throughout the vehicle's life cycle. The engineer would have to look for new technologies and designs that reduce the overall impact of a vehicle on the environment while still protecting the safety and welfare of the public.

5 Problem Solving

Problem solving is a key skill for an engineer, as engineering is mostly found on problem solving or solving an issue to make life easier/more comfortable. There is a selection of problem-solving techniques that an engineering team could employ such as value stream mapping, one-piece flow, kanban, 5-whys, Total Productive Maintenance and kaizen events(R. Keith Mobley, 2025). There are other engineering methods to help solve problems such as creating fishbone diagrams for brainstorming, Plan-Do-Check-Act (PDCA) and the failure mode and effects analysis (FMEA).

5.1 Lean Problem Solving

In the paper written by R. Keith he mentions the use of the lean method compared closely to root cause analysis (RCA). It addresses the root cause of the issue so that nothing can appear further down the production line (R. Keith Mobley, 2025). It traces the issue to its roots looking at all variables that could affect it along the way allowing engineering teams to rectify the issue after or before it arises, depending on how prepared the team is. A fishbone diagram is often used as a visual tool that helps the team group possible causes under headings such as methods, materials, machines and people as can be seen in the figure below.

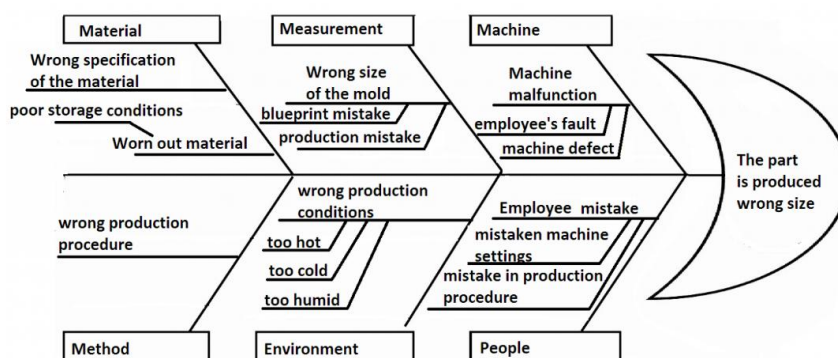


Figure 2 - Lean Fishbone Diagram (Lean Six Sigma Definition, 2020)

5.1.1 Plan-Do-Check-Act (PDCA) Method

Another common method is the PDCA method. In this method, the team first plans a way to rectify the issue and then implements it, first on a small scale. The team then checks the results and decides whether to run with the new the improvement or try a different approach. This means the team continues improvement during development. FMEA supports this by listing potential failure modes, their causes and effects, scoring the risks and prioritising actions so that high-risk issues are prevented before the product reaches customers.

Below is a visual representation of the PDCA method:

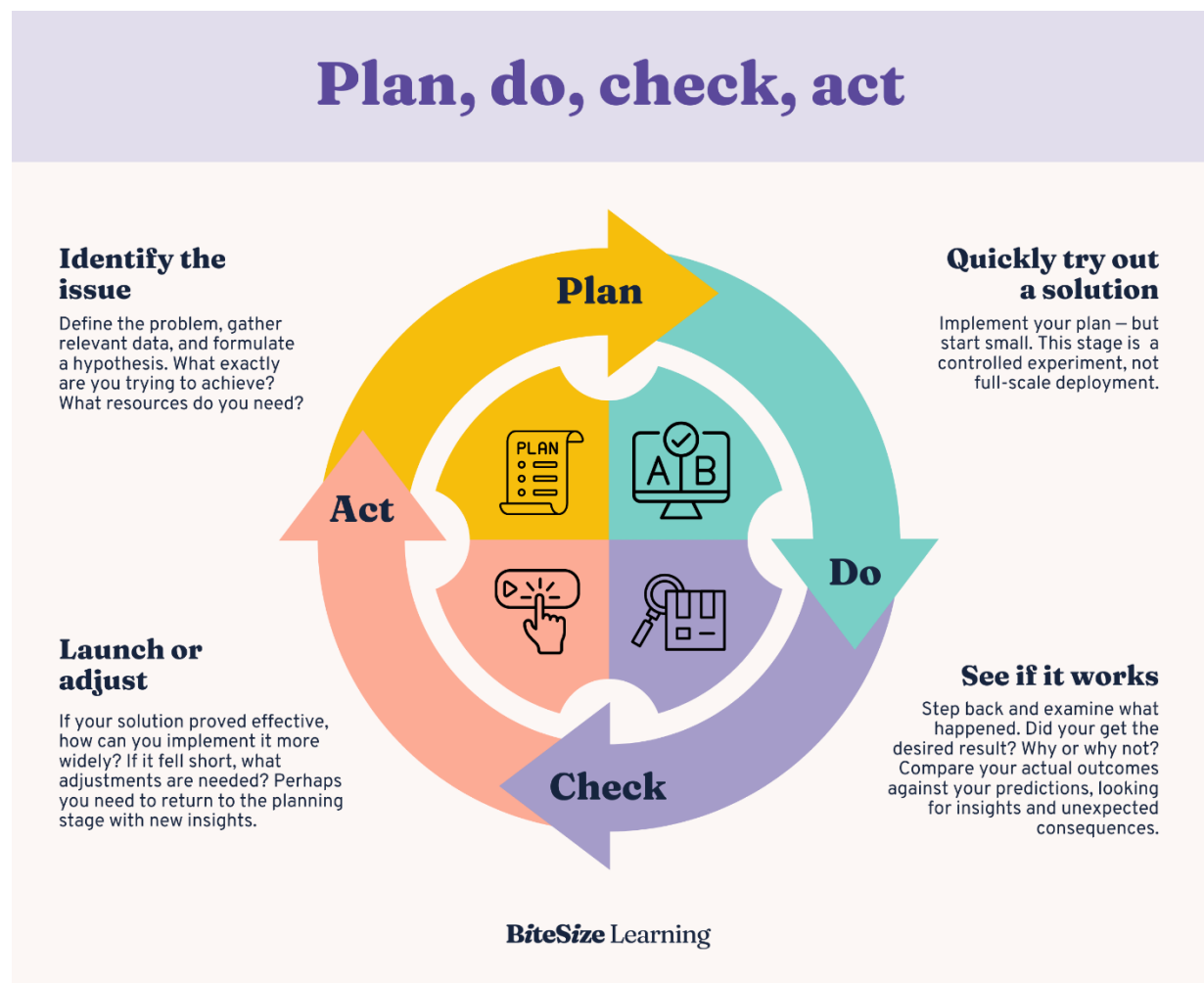


Figure 3 - Plan, Do, Check, Act (Plan, do, check, act – the PDCA cycle — BiteSize Learning, 2025)

6 Team Structure

Within the engineering industry, we often work in teams so projects can be completed efficiently and to allow for different perspectives. I have worked in a team at my previous job as a climbing instructor at Clip 'n Climb, where I worked with around six to eight people, including instructors, café staff and reception.

Whilst there my role was the team leader. Our team used a hierarchical structure. Arena staff reported to me, and I reported to the manager. If staff had an issue they could not resolve they would come to me first and if I could not fix it, I sent it up the chain. This structure had clear positives. Everyone knew who was responsible for safety and final decisions, which was crucial on the climbing arena. It also meant decisions in emergencies were made quickly because authority was obvious.

However, I also experienced several drawbacks. Communication mainly flowed top-down, and some staff felt their ideas would not be taken seriously as their ideas would get lost as they travelled up the chain. For example, I had suggestions to improve the café layout and speed up service, but I did not feel able to propose these ideas until I became team leader. Good ideas could easily be lost, depending on where they are in the hierarchy as in a case such as ours, I might find the idea pointless and as such not tell my manager (Doyle *et al.*, 2023).

An alternative that could be more effective for everyday improvements is a flatter, more participative team structure. Research suggests that structures like this can encourage joint problem solving and innovation by reducing the chain of escalation between staff (Doyle *et al.*, 2023) In my context, we could have kept clear lines of authority for safety, while using team discussions where everyone contributed ideas about operations.

7 Conclusion

This report has looked at how health and safety, risk assessments and security risks are essential in modern engineering, especially with developments like electric vehicles. It has also shown how professional conduct, problem solving methods and effective team structures all work together to help engineers protect the public, the environment and improve everyday life.

8 References

Parliament, U. (1974, 07 31). *Health and Safety at Work etc. Act 1974*. Retrieved 11 8, 2025, from <https://www.legislation.gov.uk>: <https://www.legislation.gov.uk>

Parliament, U. (1999, 12 29). *The Management of Health and Safety at Work Regulations 1999*. Retrieved 11 13, 2025, from [legislation.gov.uk](https://www.legislation.gov.uk):
<https://www.legislation.gov.uk/uksi/1999/3242/contents>

Doyle, S.P. *et al.* (2023) 'Hierarchical Team Structures Limit Joint Gain in Interteam Negotiations: The Role of Information Elaboration and Value-Claiming Behavior.', *Academy of Management Journal*, 66(5), pp. 1586–1616. Available at:
<https://doi.org/10.5465/AMJ.2019.1381>.

Ghosh, S. and Roy, T. (2025) 'Detection and isolation of battery charging cyberattacks via Koopman operator', *Applied Energy*, 401. Available at:
<https://doi.org/10.1016/j.apenergy.2025.126695>.

Institution of Engineering and Technology (2024) *RULES OF CONDUCT*. Available at:
<https://www.theiet.org/media/vj0bwbsv/rules-of-conduct-jun-2024.pdf> (Accessed: 15 November 2025).

National Society of Professional Engineers (2019) *Code of Ethics for Engineers*. Available at:
<https://www.nspe.org/sites/default/files/resources/pdfs/Ethics/CodeofEthics/NSPECodeofEthicsforEngineers.pdf> (Accessed: 15 November 2025).

Parliament, U. (1992) *Personal protective equipment (PPE) at work regulations from 6 April 2022*. Available at: <https://www.hse.gov.uk/ppe/ppe-regulations-2022.htm> (Accessed: 19 November 2025).

Parliament, U. (2002) *Control of Substances Hazardous to Health (COSHH) - HSE*. Available at: <https://www.hse.gov.uk/coshh/> (Accessed: 19 November 2025).

R. Keith Mobley (2025) *Problem-solving techniques for a high-performance team*. Available at: <https://www.reliableplant.com/Read/14690/high-performance-team> (Accessed: 17 November 2025).

Wang, F., Zhuge, C. and Chen, A. (2024) 'Data-driven vulnerability analysis of shared electric vehicle systems to cyberattacks', *Transportation Research Part D: Transport and Environment*, 135, p. 104379. Available at: <https://doi.org/10.1016/J.TRD.2024.104379>.

Automotive News (2025) 'Cyberattacks at EV charging stations are on the rise, report says', *Automotive News*, 25 February.

Jacob, R.A., Yan, M., Reynaud, J., Wolff, A. and Zhang, J. (2025) 'Cyber Attack Detection in Electric Vehicle Charging Stations Using Topological Data Aided Learning', *Proceedings of the IEEE PES General Meeting*.

Upstream Security (2024) 'EV CPO Under Siege: A New Attack Exposed the Cybersecurity and Privacy Risks of EV Charging Networks'.