

				Severity					
				5	4	3	2	1	0
				Apocalyptic	Catastrophic	Serious	Major	Marginal	Minor
Likelihood	5	Frequent	1×10^{-1}	1	1	1	2	3	4
	4	Probable	1×10^{-2}	1	2	2	3	4	4
	3	Occasional	1×10^{-3}	1	2	3	4	4	5
	2	Remote	1×10^{-6}	1	2	3	4	4	5
	1	Improbable	1×10^{-9}	1	3	4	4	5	5
	0	Incredible	1×10^{-12}	2	3	4	5	5	5

Hazard ID	Hazard	Hazard Description	Accident	Cause	Cause Description	Severity		Likelihood	Risk Class	Controls and/or Mitigations	C&M		
						(highest)					Severity	applied likelihood	C&M applied Risk Class
Hazard 01	Moving parts - powered hatches and doors	The potential for appendages to become caught in / trapped in / collide with hatches or doors that can shut with a high amount of force and pressure	Appendage caught in / trapped in may lead to: • Major Injury of DIRECT PERSONNEL such as limb loss due to force and pressure	Human Error	The operator does not follow intended operating procedure leaving appendages in line with the moving parts of the hatches or doors	Major		Probable (10^-2)	3	• Appropriate training for personnel who operate the doots and hatches. • PPE to help mitigate any injury from operational errors.	Major	Occasional (10^-3)	4
			Appendage Collides with may lead to: • Minor injury of DIRECT PERSONNEL such as concussion due to force	Electronic Failure	Electronic failure could lead to the hatch or door closing unexpectedly while an object is obstructing its path.	Major		Remote (10^-6)	4	• Sensors to detect door and hatch obstruction. • Ensure the design of the electronic and mechanical systems meet the failue rate standards. For example ISO13849 - Safety of Machinery or similiar standard of choice.	Major	Remote (10^-6)	4
				Mechanical Failure	Mechanical failure could lead to the hatch or door closing unexpectedly while an object is obstructing its path.	Major		Remote (10^-6)	4	• Design door and hatch operation such that it is difficult to operate without any appendages being free to obstruct the closing path.	Major	Remote (10^-6)	4
Hazard 02	Hatch / Door Failure	Potential for operators to become permanently sealed inside vehicle	Door or Hatch becoming unable to open and prevent egress may cause fatality of DIRECT PERSONNEL due to inability to exit vehicle during fire	Electronic / Mechanical Failure due to design	Mechanical and / or Electronic failure prevents operation.	Catastrophic		Remote (10^-6)	2	• Implement manual opening system that does not rely on electronic or mechanical assistance on the inside of the vehicle. • Ensure the design of the electronic and mechanical systems meet the failue rate standards. For example ISO13849 - Safety of Machinery or similiar standard of choice.	Catastrophic	Improbable (10^-9)	3
				Electronic / Mechanical failure due to damage from attack	Damage from an attack to the system prevents operation	Catastrophic		Frequent (10^-1)	1	• Have more than one option for egress that does not rely on electronic or mechanical mechanisms.	Catastrophic	Improbable (10^-9)	3

Hazard 03	Heavy Vehicle	A heavy vehicle capable of around 45 mph collides with people or object	Collision / Crushing may cause fatality of multiple INDIRECT PERSONNEL	Human Error	General error in operation or factors such as fatigue, combat stress or unfamiliar situation result in a collision.	Catastrophic	Probable (10 ⁻²)	2	• Ensure operators are well trained in the operation of the vehicle. • Ensure operators are frequently exposed to drills that emulate sabotage and interference scenarios. • Implement failsafe breaking system disconnected from main breaking system in case of mechanical failure. • Provide operator with systems in the vehicle capable of combating enemy interference such as IR scope to see through smoke screen. • Implement automated system that detects objects close to the vehicle in all directions to reduce chance of accidentally crushing personnel.	Catastrophic	Occasional (10 ⁻³)	2
				Mechanical Failure	Mechanical systems governing vehicle control fail and result in a collision	Catastrophic	Remote (10 ⁻⁶)	2		Catastrophic	Improbable (10 ⁻⁹)	3
			Collision with object may cause major injury to DIRECT PERSONNEL	Sabotage / Interference	Enemy uses means of interfering with the vehicle systems that provide the operator with visibility of their surroundings	Catastrophic	Probable (10 ⁻²)	2		Catastrophic	Remote (10 ⁻⁶)	2
Hazard 04	Inadvertant detonation of 40 mm HE munition	The potential for munition high explosive (HE) to undergo detonation during operational conditions despite not undergoing the	Detonation while stored on platform may lead to fatality of DIRECT PERSONNEL inside the vehicle	Failure of fuzing / safety and arming unit	Failure of the safety and arming unit such as arming early and the fuze becomes in line with the HE completing the explosive initiation train	Catastrophic	Remote (10 ⁻⁶)	2	• Refer to the guidance in DSA.03 OME DCOP 107 that points to standards for qualifying the explosives materials i.e STANAG 4170 and AOP-07. Within there is a section on vulnerability / Insensitive munitions, select a HE fill which scores strongly against vulnerabilities so that it is not sensitive to heat, impact, Electromagnetic interference and fragment penetration. • Have at least a 2 point	Catastrophic	Improbable (10 ⁻⁹)	3
			Early detonation during flight to target may lead to fatality of INDIRECT PERSONNEL	Exposure to Electromagnetic Radiation	Powerful electromagnetic radiation waves provides credible energy stimulus to	Catastrophic	Remote (10 ⁻⁶)	2		Catastrophic	Improbable (10 ⁻⁹)	3

	mm HE munition	not undergoing the designed arming process and receiving the correct detonation stimuli		Shock / Heat / Fragment insult from enemy munition	Shock / Heat / Fragment insult provides credible energy stimulus to initiate explosive	Catastrophic	Probable (10 ⁻²)	2	safety system for the SAU so that if one fails there is a backup to keep the system safe. • Ensure the SAU has a minimum distance / time to activate after firing to reduce the probability of friendly fire. • Perform drills that emulate situations that would be encountered during operation to train the operators.	Catastrophic	Improbable (10 ⁻⁹)	3
				Human Error	Target settings leads to friendly fire	Catastrophic	Probable (10 ⁻²)	2		Catastrophic	Occasional (10 ⁻³)	2
				Exposure to very high temperature environment	Heat from events on the battlefield provides credible energy stimulus to initiate the explosive	Catastrophic	Probable (10 ⁻²)	2		Catastrophic	Improbable (10 ⁻⁹)	3
Hazard 05	L94A1 coaxial 7.62 mm chain gun	A device capable of emitting multiple large high velocity projectiles over a short period of time	Friendly fire may occur during operations leading to fatality of INDIRECT PERSONNEL	Human Error	Operator error leads to friendly fire	Serious	Probable (10 ⁻²)	2	• Perform drills that emulate situations that would be encountered during operation to train the operators. • Provide a means of safely unloading the weapon while its firing in the event of a mechanical failure. • Provide operators with multiple means of targetting that are capable of combating different types of enemy interference such as IR targetting to combat enemy smoke screen.	Serious	Occasional (10 ⁻³)	3
				Mechanical Failure	Mechanical failure results in unintended discharge of munition	Serious	Remote (10 ⁻⁶)	3		Serious	Improbable (10 ⁻⁹)	4
				Sabotage / Interference	Sabotage / interference from enemy causes an error in identifying friend from foe	Serious	Probable (10 ⁻²)	2		Serious	Remote (10 ⁻⁶)	3

UWTSD

ACDB 5013: ALARP Justification

Alun Morris

Contents

Overview – The Environment and Munition.....	3
The Door and Hatch System	3
Hazard 01 - Hazard Identification	3
Hazard 01 - Hazard Causation.....	3
Hazard 01 - Controls and Mitigation.....	4
Hazard 01 – ALARP Justification.....	5
References:	7

Academic integrity declaration

I declare that:

- the assignment submitted has been written by me alone.
- the assignment submitted has not been previously submitted to this university or any other.
- that all content, including primary and/or secondary data, is true to the best of my knowledge.
- that all quotations and references have been duly acknowledged according to the requirements of academic research.

I understand that to knowingly submit work in violation of the above statement will be considered by examiners as academic misconduct.

Overview – The Environment and Munition

This document will be justifying the controls and mitigations presented in the attached Ajax risk assessment for Hazard ID: Hazard 01 – Moving parts powered doors and hatches.

The Ajax is a technologically advanced medium armoured fighting vehicle offering survivability, mobility and is equipped with an advanced sensor suite [1]. There are several variations of the AJAX with each version supporting the powered door and hatch system. “Powered” in this report is a catch-all term that encompasses both mechanical assistance (e.g., hydraulic systems) and electrical assistance (e.g., power from a source such as a battery). The AJAX can be crewed by up to 3 operators.

The risk assessment was created for the scenario of the vehicle being deployed on operations against a hostile force. Therefore, it is assumed in the risk assessment that the probability of human error would be higher than under non combative circumstances. HSE guidance and their study on human error and behaviour [2] support this assumption.

The Door and Hatch System

Point of ingress and egress on an armoured fighting vehicle must be sufficiently robust to withstand the threats the vehicle is designed to protect against otherwise they would become vulnerabilities in the systems design. To meet this requirement the doors and hatches are armoured, and as a result are heavy. They must also be able to seal tightly to prevent or reduce the contamination of the air inside the vehicle when the hatch is closed.

Due to the weight of the hatch manually operating the hatch system could cause difficulty for the operator. To address this, the hatch closing mechanism is supported by vehicle hydraulics, with the actuation controlled by an electrical system.

Operators are expected to interact with the system frequently during deployment. Performing a visual reconnaissance of the environment by emerging from the inside of the vehicle when conditions allow can provide valuable data that the sensor system may be unable to satisfy.

Hazard 01 - Hazard Identification

The predominant hazard associated with the moving components of the door and hatch system is the potential for **major injury to direct personnel**, resulting from **crushing or severing of appendages** due to the significant **hydraulic forces involved during hatch closure**.

To demonstrate that this risk has been reduced to ALARP, in accordance with Ministry of Defence (MOD) safety principles, the duty holder must identify the individual with the greatest exposure to the hazard [3]. For this system, the operator of the hatch is the most at risk, as other vehicle personnel are unlikely to interact with the hatch during its closing operation.

Hazard 01 - Hazard Causation

The identified causes contributing to the hazard of major injury to direct personnel during hatch closure include:

- **Human Error** - The operator unintentionally initiates hatch closure while an appendage is positioned across the hatch threshold.
- **Mechanical Failure** - Malfunction of the hydraulic system results in abrupt or uncontrolled hatch movement.
- **Electronic Failure** - Errors in control system logic trigger unintended hatch actuation.

- **Sensor Failure** - Failure of position or obstruction sensors prevents the system from detecting personnel presence or identifying obstructions in the hatch path.

Hazard 01 - Controls and Mitigation

When designing the controls and mitigation measures it was vital to consider that the powered hatch system must remain operable and safe in environments influenced by WOME hazards such as shock, blast wave propagation, and electromagnetic interference from nearby ordnance detonation. The controls and mitigations implemented ensure resilience against these influences without introducing disproportionate complexity or compromising mission capability.

Human Error:

In the accompanying qualitative risk assessment for the AJAX platform human error was identified as the dominant risk with an estimated likelihood of 1×10^{-2} to reduce the probability of a major accident arising from this hazard the following controls and mitigations have been implemented:

- **Procedural Control:**
To reduce the likelihood of an appendage being positioned across the hatch threshold actuation of the hatch requires two hands to operate. In the HAZOP method outlined in the HSE guidance and in the journal "A PRACTICAL APPLICATION OF 'HUMAN-HAZOP' FOR CRITICAL PROCEDURES" by G. Ellis and A. Holt step 6 assess risk reduction methods asks the question of can the hazard be removed by applying an inherently safe design? [4]. While this control may not remove the hazard entirely due to operational constraints, it can reasonably be argued to reduce the risk.
- **Procedural Control:**
Platform operators regularly undertake drills simulating the operational combat environment, helping to reduce the likelihood of human error under stress.
- **Mitigation:**
A visual and audio indicator is positioned directly in the operator's line of sight. This indicator is activated by a hatch-mounted sensor that detects obstructions and prevents closure when unsafe conditions are present.
- **Mitigation:**
Personal Protective Equipment such as helmet and gloves can be worn to mitigate any minor injuries that may occur from the hazard such as collision with the hatch as it closes or a minor pinch. However, it is unlikely to protect against the crushing forces resulting from direct obstruction.

Despite these controls and mitigations, considering the nature of the operational combat environment combined with the inherent proclivity of human error especially in high stress environments makes it unreasonable to assert the risk is completely mitigated. Based on a qualitative assessment, it is assumed for the purposes of this report that the likelihood of an accident is reduced to 1×10^{-3} post-mitigation.

Mechanical Failure:

The following controls and mitigations implemented:

- **Control:**
Designed to the appropriate standards of DefStan 23-7 Design Guidelines for Armoured Fighting Vehicles and ISO 4413 Hydraulic Fluid Power.
- **Control:**

Sensor system that detects obstruction positioned across the hatch closing threshold.

- **Control:**
Regular maintenance of the system prior to and after operations.
- **Mitigation:**
Hydraulic accumulator included in the system as recommended in “*Case Study and Critical analysis to find the FMEA in Hydraulics System*” [5] to act as a failsafe in the unlikely event of a system failure.

With the controls and mitigations in place a qualitative assessment of the risk is remote. It is recommended that a quantitative assessment is performed to strengthen the ALARP argument.

Electronic Failure and Sensor failure:

The following controls and mitigations implemented:

- **Control:**
Designed to the guidance in DSA OME.03 DCOP 109 Defence Code of Practice for Software and Programmable Hardware and DefStans 00-055: *Requirements for Safety of Programmable Elements in Defence Systems*, 00-056: *Safety Management Requirements for Defence Systems* and 59-411: *Electromagnetic Compatibility (EMC)*
- **Control:**
Regular maintenance of the system prior to and after operations.
- **Mitigation:**
Ensure hatch returns to a safe open state in the event a failure is detected.
- **Mitigation:**
In the event of failure and the hatch is defaulted to open state there is a manual closing system to enable the operator to close the hatch if they are under duress from hostiles.

With the controls and mitigations in place a qualitative assessment of the risk is remote. It is recommended that a quantitative assessment is performed to strengthen the ALARP argument.

Hazard 01 – ALARP Justification

The likelihood of failure for the mechanical, electrical, and sensor components of the hydraulic hatch system is assessed as *remote* over a 20-year service life under combat conditions. The potential accident of a major injury to a single operator has been evaluated within the system’s safety framework.

This risk is considered **ALARP** because additional failsafe mechanisms would require substantial space trade-offs in the vehicle’s internal layout. Given the hatch’s compliance with DefStan 23-7 and ISO 4413, and the inclusion of control measures such as sensors and hydraulic accumulators, the residual risk does not justify disproportionate mitigation. Space is better allocated to systems essential for vehicle combat effectiveness.

Human error is identified as the dominant risk to the system, with the highest likelihood of causing a major accident to the operator. Mitigation measures were considered to reduce the severity of injury including the development of bespoke glove PPE capable of withstanding the closing force of the hatch and preventing hand crushing or severance. One control option explored was the use of an armoured hatch seal made from a malleable polymer that, while resistant to shock, fragmentation, and heat, would deform under pressure, allowing the operator’s appendages to slide free safely as the hatch sealed. However, based on the following Cost Benefit Analysis (CBA) formula:

$$\text{Grossly Disproportionate Cost} = VPF \times [P1 \times GDF1 - P2 \times GDF2]$$

Equation 1 - Cost Benefit Analysis Post Mitigation

VPF = Value of prevented fatality/injury/harm = £207,200

P1 = Initial Probability of accident under review, per year = 1×10^{-3}

GDF1 = Initial Grossly Disproportionate Factor = 5

P2 = Post Mitigation Probability of accident under review, per year = 1×10^{-3}

GDF2 = Post Mitigation Grossly Disproportionate Factor = 5

The probability figures were defined from the qualitative risk assessment. The VPF is using numbers established by the Health and Safety Executive (HSE) and the GDF for this report was decided at 5 for a major injury and 3 for a minor injury, this data was extrapolated from looking at the table A1.2 - Technical Note on Proportion Factors by ERM, 2009[6] and making a judgment for an operator in a combat environment where a major injury is potentially operation ending and even a minor injury could result in consequences to life and success of the operation.

Using this equation to calculate the Grossly Disproportionate cost for reducing the severity of the accident from major to minor equals a cost of anything over £414 being disproportionate. Since the research and development costs alone would far exceed £414 for bespoke PPE and a malleable polymer that is resistant enough to not pose a vulnerability to the system. Considering the CBA on reducing the risk further it is justified that the current measures implemented are ALARP. However, should the technology become cheaper it may warrant re-evaluation in future safety reviews.

This ALARP justification is a live document and should be revisited if any of the following occur: changes to system configuration, publication of a detailed quantitative risk assessment, shifts in operational doctrine, or reductions in the cost of relevant technologies.

References:

- [1] "Ajax | The British Army," *Army.mod.uk*, 2024. <https://www.army.mod.uk/learn-and-explore/equipment/combat-vehicles/ajax/>
- [2] Health And Safety Executive, *Reducing error and influencing behaviour*. Sudbury: Hse Books, Cop, 1999.
- [3] "An Introduction to System Safety Management in the MOD PART I System Safety Concepts and Principles," 2018. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/904238/SSM_Whitebook_PART_1_2020_update_2.pdf
- [4] G. Ellis and A. Holt, "A PRACTICAL APPLICATION OF 'HUMAN-HAZOP' FOR CRITICAL PROCEDURES." Accessed: Jan. 01, 2020. [Online]. Available: <https://www.icheme.org/media/9560/xxi-paper-063.pdf>
- [5] C. Johny and K. Rsivadas, "Case Study and Critical analysis to find the FMEA in Hydraulics System." Accessed: Jul. 14, 2025. [Online]. Available: <https://www.iosrjournals.org/iosr-jmce/papers/ICETEM/Vol.%201%20Issue%203/36-60-66.pdf>
- [6] L. Guen and G. Produced, "ANNEX 1: Guidance on Proportion Factors A1.1 -Work by RAPU and ESAU." Accessed: Jul. 14, 2025. [Online]. Available: https://www.hse.gov.uk/foi/internalops/hid_circs/permissioning/spc_perm_37/annex1.pdf

