I. Filled OCTAVE Worksheets

Allegro – Worksheet 10		**R1 – Jamming ultrasonic sensors**					
Threat	**Business Asset**	Ultrasonic sensors data					
	Business Asset's Value	Low – Losing ultrasonic sensors data does not impact BOLT AV					
	Area of Concern	An attacker uses ultrasonic frequency emitter to manipulate the data received by the sensors causing false blackout by the sensors and loss of integrity of Ultrasonic sensors data.					
	Actor *Who would exploit the area of concern or threat?*	An attacker with some previous experience with ultrasound sensors. Has a DIY ultrasonic jammer.					
	Means *How would the actor do it? What would they do?*	An attacker uses their knowledge and tools to carry out a jamming attack on ultrasonic ranging sensors by emitting frequencies used by the sensors and causing false information received by the sensor.					
	Motive *What is the actor's reason for doing it?*	Wants disrupt the AV program to keep drivers' jobs.					
	Outcome (choose one) *What would be the resulting effect be?*	Disclosure:		Destruction:			
		Modification:		Interruption:	x		
	Security Requirements *How would the information asset's security requirements be breached?*	Ultrasonic sensors are not jamming resistant.					
	Likelihood (choose one)	High:		Medium:	x	Low:	

Consequences *What are the consequences to the organization as a result of the risk?*	**Severity** *How severe are the consequences to the organization or asset owner by impact area?* **3 for highest priority, 2 for medium and 1 for lowest*			
Losing the integrity of data will cause the system to make wrong decisions and potential harm to other road users. Not having the sensor available without any mitigations will cause the system to not see the outside, possibly other sensors can cover. Jamming attack on ultrasonic sensor will not cause any data leaks.	Impact area	Priority*	Impact	Score
	Confidentiality	1	Low	1
	Availability	2	High	6
	Integrity	3	High	9

Relative risk score:	**16**
Total Risk Score *(Rel x likelihood):*	**32**

Risk Mitigation	**R1 – Jamming ultrasonic sensors**							
Choose action to take.	Accept:		Defer:		Mitigate:	x	Transfer:	
For the risk, what actions and controls will be used:								

Layer where applied	**Description of control or action**	**Estimated cost**
Perception	Noise detection and rejection	Low
Perception	Multiple sensors for redundancy check	Low

Allegro – Worksheet 10		**R2 – Spoofing ultrasonic sensors**					
Threat	**Business Asset**	Ultrasonic sensors data					
	Business Asset's Value	Low – Losing ultrasonic sensors data does not impact BOLT AV					
	Area of Concern	An attacker uses ultrasonic frequency emitter with crafted pulse to manipulate the data received by the sensors causing false information received by the sensors and loss of integrity of measurement data.					
	Actor *Who would exploit the area of concern or threat?*	An attacker with some previous experience with ultrasound sensors. Has a DIY ultrasonic emitter.					
	Means *How would the actor do it? What would they do?*	An attacker uses their knowledge and tools to carry out a spoofing attack on ultrasonic ranging sensors by emitting carefully crafted frequencies and sequences causing false information received by the sensor.					
	Motive *What is the actor's reason for doing it?*	Wants disrupt the AV program to keep drivers' jobs.					
	Outcome (choose one) *What would be the resulting effect be?*	Disclosure:		Destruction:			
		Modification:	x	Interruption:			
	Security Requirements *How would the information asset's security requirements be breached?*	Ultrasonic sensors are not spoofing resistant.					
	Likelihood (choose one)	High:		Medium:	x	Low:	

Consequences *What are the consequences to the organization as a result of the risk?*	**Severity** *How severe are the consequences to the organization or asset owner by impact area?* **3 for highest priority, 2 for medium and 1 for lowest*			
Losing the integrity of data will cause the system to make wrong decisions and potential harm to other road users. Not having the sensor available without any mitigations will cause the system to not see the outside, possibly other sensors can cover. Spoofing attack on ultrasonic sensor will not cause any data leaks.	Impact area	Priority*	Impact	Score
	Confidentiality	1	Low	1
	Availability	2	High	6
	Integrity	3	High	9

Relative risk score:	**16**
Total Risk Score *(Rel x likelihood):*	**32**

Risk Mitigation	**R2 – Spoofing ultrasonic sensors**							
Choose action to take.	Accept:		Defer:		Mitigate:	x	Transfer:	
For the risk, what actions and controls will be used:								

Layer where applied	**Description of control or action**	**Estimated cost**
Perception	Noise detection and rejection	Low
Perception	Multiple sensors for redundancy check	Low

Allegro – Worksheet 10		**R3 – Acoustic quieting**					
Threat	**Business Asset**	Ultrasonic sensors data					
	Business Asset's Value	Low – Losing ultrasonic sensors data does not impact BOLT AV					
	Area of Concern	An attacker uses sound absorbing materials to cover some objects to make them hard to detect by the sensors causing late detection (possible collisions) and loss of integrity of measurement data.					
	Actor *Who would exploit the area of concern or threat?*	An attacker with some previous experience with ultrasound sensors. Has sound absorbing materials to use.					
	Means *How would the actor do it? What would they do?*	An attacker uses their knowledge and materials to cover nearby objects to make them harder to detect with ultrasound sensors which causes late detections.					
	Motive *What is the actor's reason for doing it?*	Wants disrupt the AV program to keep drivers' jobs.					
	Outcome (choose one) *What would be the resulting effect be?*	Disclosure:		Destruction:			
		Modification:		Interruption:	x		
	Security Requirements *How would the information asset's security requirements be breached?*	Ultrasonic sensors are not acoustic quieting resistant.					
	Likelihood (choose one)	High:		Medium:		Low:	x

Consequences *What are the consequences to the organization as a result of the risk?*	**Severity** *How severe are the consequences to the organization or asset owner by impact area?* **3 for highest priority, 2 for medium and 1 for lowest*			
Acoustic quieting will hide some objects from the ultrasonic ranging device. Not seeing possible obstacles can cause traffic accidents and harm to people and other property. The sensors will still work, only their data cannot be trusted when acoustic quieting is detected as some objects are hidden. No data leaks will be caused by acoustic quieting .	Impact area	Priority*	Impact	Score
	Confidentiality	1	Low	1
	Availability	2	Low	2
	Integrity	3	High	9
	Relative risk score:			**12**
	Total Risk Score *(Rel x likelihood):*			**12**

Risk Mitigation	**R3 – Acoustic quieting**							
Choose action to take.	Accept:		Defer:		Mitigate:	x	Transfer:	
For the risk, what actions and controls will be used:								
Layer where applied	**Description of control or action**					**Estimated cost**		
Perception	Multiple sensors for redundancy check					Low		

Allegro – Worksheet 10		**R4 – Jamming radar**					
Threat	**Business Asset**	Surrounding environment data					
	Business Asset's Value	High – Without Surrounding environment data, car cannot continue					
	Area of Concern	An attacker uses their tools to manipulate the data received by the radar causing false blackout on the radar and loss of integrity of surrounding environment data.					
	Actor *Who would exploit the area of concern or threat?*	An attacker with some previous experience with radars and has signal generator (+multiplier etc.).					
	Means *How would the actor do it? What would they do?*	An attacker uses their knowledge and tools to carry out a jamming attack on radar by emitting frequencies used by the sensors and causing false information (distance constantly changing) received (76-77GHz in the experiment).					
	Motive *What is the actor's reason for doing it?*	Wants disrupt the AV program to keep drivers' jobs.					
	Outcome (choose one) *What would be the resulting effect be?*	Disclosure:		Destruction:			
		Modification:		Interruption:	x		
	Security Requirements *How would the information asset's security requirements be breached?*	Radars are not jamming resistant.					
	Likelihood (choose one)	High:		Medium:	x	Low:	

Consequences *What are the consequences to the organization as a result of the risk?*	**Severity** *How severe are the consequences to the organization or asset owner by impact area?* **3 for highest priority, 2 for medium and 1 for lowest*			
Losing the integrity of data will cause the system to make wrong decisions and potential harm to other road users. Not having the sensor available without any mitigations will cause the system to not see the outside, possibly other sensors can cover. Jamming attack on radar will not cause any data leaks.	Impact area	Priority*	Impact	Score
	Confidentiality	1	Low	1
	Availability	3	High	9
	Integrity	2	High	6

Relative risk score:	**16**
Total Risk Score *(Rel x likelihood):*	**32**

Risk Mitigation	**R4 – Jamming radar**						
Choose action to take.	Accept:		Defer:		Mitigate:	x	Transfer:

For the risk, what actions and controls will be used:

Layer where applied	**Description of control or action**	**Estimated cost**
Perception	Noise detection and rejection	Low
Perception	Multiple sensors for redundancy check	Low

Allegro – Worksheet 10		**R5 – Spoofing radar**					
Threat	**Business Asset**	Surrounding environment data					
	Business Asset's Value	High – Without Surrounding environment data, car cannot continue					
	Area of Concern	An attacker uses their tools to manipulate the data received by the radar causing constant changes in distance/velocity on the radar and loss of integrity of surrounding environment data.					
	Actor *Who would exploit the area of concern or threat?*	An attacker with some previous experience with radars and has signal generator (+multiplier etc.).					
	Means *How would the actor do it? What would they do?*	An attacker uses their knowledge and tools to carry out a spoofing attack on radar by emitting frequencies used by the sensors and causing false information (no objects detected) received (76-77GHz in the experiment)					
	Motive *What is the actor's reason for doing it?*	Wants disrupt the AV program to keep drivers' jobs.					
	Outcome (choose one) *What would be the resulting effect be?*	Disclosure:		Destruction:			
		Modification:		Interruption:	x		
	Security Requirements *How would the information asset's security requirements be breached?*	Radars are not spoofing resistant.					
	Likelihood (choose one)	High:		Medium:	x	Low:	

Consequences *What are the consequences to the organization as a result of the risk?*	**Severity** *How severe are the consequences to the organization or asset owner by impact area?* **3 for highest priority, 2 for medium and 1 for lowest*			
Losing the integrity of data will cause the system to make wrong decisions and potential harm to other road users. Not having the radar available without any mitigations will cause the system to not see the outside, possibly other sensors can cover. Spoofing attack on radar will not cause any data leaks.	Impact area	Priority*	Impact	Score
	Confidentiality	1	Low	1
	Availability	2	High	6
	Integrity	3	High	9
			Relative risk score:	**16**
			Total Risk Score *(Rel x likelihood):*	**32**

Risk Mitigation	**R5 – Spoofing radar**							
Choose action to take.	Accept:		Defer:		Mitigate:	x	Transfer:	
For the risk, what actions and controls will be used:								

Layer where applied	**Description of control or action**	**Estimated cost**
Perception	Noise detection and rejection	Low
Perception	Multiple sensors for redundancy check	Low

Allegro – Worksheet 10		**R6 – Blinding attack on cameras**					
Threat	**Business Asset**	video and image data					
	Business Asset's Value	Medium – Car can continue driving but can't recognize signs and traffic lights.					
	Area of Concern	An attacker uses their tools to send malicious optical data to the camera causing unwanted blindness, possible hardware damage and loss of integrity of video and image data.					
	Actor *Who would exploit the area of concern or threat?*	An attacker with some previous experience and tools to send malicious optical inputs (laser etc.).					
	Means *How would the actor do it? What would they do?*	An attacker uses their knowledge and malicious optical emitters to send and blind cameras causing unwanted blindness on the cameras and possibly permanently damage the camera sensors.					
	Motive *What is the actor's reason for doing it?*	Wants disrupt the AV program to keep drivers' jobs.					
	Outcome (choose one) *What would be the resulting effect be?*	Disclosure:		Destruction:			
		Modification:		Interruption:	x		
	Security Requirements *How would the information asset's security requirements be breached?*	Cameras are vulnerable to blinding attacks.					
	Likelihood (choose one)	High:	x	Medium:		Low:	

Consequences *What are the consequences to the organization as a result of the risk?*	**Severity** *How severe are the consequences to the organization or asset owner by impact area?* **3 for highest priority, 2 for medium and 1 for lowest*			
Blinding attack will cause some blind spots on the image recorded by the cameras. Blind spots can cause not detecting objects and possible accidents because of that. Not having the sensor available without any mitigations will cause the system to not see the outside, possibly other sensors can cover. Using lasers to carry out the attack can permanently damage the camera's lens..	Impact area	Priority*	Impact	Score
	Confidentiality	1	Low	1
	Availability	3	High	9
	Integrity	2	High	6
			Relative risk score:	**16**
			Total Risk Score *(Rel x likelihood):*	**48**

Risk Mitigation	**R6 – Blinding attack on cameras**							
Choose action to take.	Accept:		Defer:		Mitigate:	x	Transfer:	
For the risk, what actions and controls will be used:								

Layer where applied	**Description of control or action**	**Estimated cost**
Perception	Overlapping image output with multiple cameras	Low
Perception	Filter to remove harmful light	High

Allegro – Worksheet 10		**R7 – Confusing controls with attack on cameras**
Threat	**Business Asset**	Video and Image data
	Business Asset's Value	Medium – Car can continue driving but can't recognize signs and traffic lights
	Area of Concern	An attacker uses their tools to send malicious optical short output and blind cameras causing unwanted blindness and confusion for longer period, possible hardware damage and loss of integrity of video and image data.
	Actor *Who would exploit the area of concern or threat?*	An attacker with some previous experience and tools to send malicious optical inputs (laser etc.), tools to further destabilize the input.
	Means *How would the actor do it? What would they do?*	An attacker uses their knowledge and malicious optical emitters to send a short output and blind cameras causing unwanted blindness and confusion for longer period on the cameras and possibly permanently damage the camera sensors
	Motive *What is the actor's reason for doing it?*	Wants disrupt the AV program to keep drivers' jobs.
	Outcome (choose one) *What would be the resulting effect be?*	
	Security Requirements *How would the information asset's security requirements be breached?*	Cameras are vulnerable to blinding attacks.
	Likelihood (choose one)	

Disclosure:		Destruction:	
Modification:		Interruption:	x

High:		Medium:	x	Low:	

Consequences *What are the consequences to the organization as a result of the risk?*	**Severity** *How severe are the consequences to the organization or asset owner by impact area?* **3 for highest priority, 2 for medium and 1 for lowest*
Blinding attack will cause some blind spots on the image recorded by the cameras. Blind spots can cause not detecting objects and possible accidents because of that. The blindness stays for longer as the input is optimized. Not having the sensor available without any mitigations will cause the system to not see the outside, possibly other sensors can cover. Using lasers to carry out the attack can permanently damage the camera's lens.	

Impact area	Priority*	Impact	Score
Confidentiality	1	Low	1
Availability	3	High	9
Integrity	2	High	6

Relative risk score:	**16**
Total Risk Score *(Rel x likelihood):*	**32**

Risk Mitigation	**R7 – Confusing controls with attack on cameras**	
Choose action to take.	Accept: □ Defer: □ Mitigate: x Transfer: □	
For the risk, what actions and controls will be used:		
Layer where applied	**Description of control or action**	**Estimated cost**
Perception	Overlapping image output with multiple cameras	Low
Perception	Filter to remove harmful light	High

Allegro – Worksheet 10		**R8 – Relay attack on LiDAR**
Threat	**Business Asset**	Surrounding environment data
	Business Asset's Value	High – Without Surrounding environment data, car cannot continue
	Area of Concern	An attacker uses their tools to send a light wave and manipulating the information got by the LIDAR to carry out the relay attack causing confusion, errors and loss of integrity of surrounding environment data.
	Actor *Who would exploit the area of concern or threat?*	An attacker with some previous experience and tools to send light with specific (905nm) wavelengths, oscilloscope.
	Means *How would the actor do it? What would they do?*	An attacker uses their knowledge and tools to carry out a relay attack confusing and manipulating the data received by the LIDAR causing unwanted errors
	Motive *What is the actor's reason for doing it?*	Wants disrupt the AV program to keep drivers' jobs.

Outcome (choose one) *What would be the resulting effect be?*	Disclosure:		Destruction:	
	Modification:	x	Interruption:	

Security Requirements *How would the information asset's security requirements be breached?*	LIDAR's are not relay attack resistant.

Likelihood (choose one)	High:		Medium:		Low:	x

Consequences *What are the consequences to the organization as a result of the risk?*	**Severity** *How severe are the consequences to the organization or asset owner by impact area?* **3 for highest priority, 2 for medium and 1 for lowest*			
Relay attack will manipulate with the data gathered by the LiDAR. This causes errors in the system and possible accidents in the traffic. Unhandled errors can cause shutdown of the LiDAR. Confidentiality is unaffected.	Impact area	Priority*	Impact	Score
	Confidentiality	1	Low	1
	Availability	3	High	6
	Integrity	3	High	9

Relative risk score:	**16**
Total Risk Score *(Rel x likelihood):*	**16**

Risk Mitigation	**R8 – Relay attack on LiDAR**							
Choose action to take.	Accept:		Defer:		Mitigate:	x	Transfer:	

For the risk, what actions and controls will be used:

Layer where applied	**Description of control or action**	**Estimated cost**
Perception	Multiple LiDAR inputs	High
Perception	Random probing	Low
Perception	Shorten pulse period	Low

Allegro – Worksheet 10		**R9 – Spoofing LiDAR**					
Threat	**Business Asset**	surrounding environment data					
	Business Asset's Value	High – Without Surrounding environment data, car cannot continue					
	Area of Concern	An attacker uses their knowledge and tools to create objects for LIDAR in the environment, that are not there and causing loss of integrity of surrounding environment data.					
	Actor *Who would exploit the area of concern or threat?*	An attacker with some previous experience and tools to send light with specific (905nm) wavelengths, oscilloscope.					
	Means *How would the actor do it? What would they do?*	An attacker uses their knowledge and tools to create objects for LIDAR in the environment, that are not there.					
	Motive *What is the actor's reason for doing it?*	Wants disrupt the AV program to keep drivers' jobs.					
	Outcome (choose one) *What would be the resulting effect be?*	Disclosure:		Destruction:			
		Modification:		Interruption:	x		
	Security Requirements *How would the information asset's security requirements be breached?*	LIDAR's are not spoofing resistant.					
	Likelihood (choose one)	High:		Medium:		Low:	x

Consequences *What are the consequences to the organization as a result of the risk?*	**Severity** *How severe are the consequences to the organization or asset owner by impact area?* **3 for highest priority, 2 for medium and 1 for lowest*			
Creating artificial objects seen by the LiDAR will cause unwanted errors in the systems driving management and could lead to traffic interruptions and accidents. Impact on availability is there, but the attack does not remove real objects and only adds new artificial ones. Confidentiality is not affected.	Impact area	Priority*	Impact	Score
	Confidentiality	1	Low	1
	Availability	2	Medium	4
	Integrity	3	High	9

Relative risk score:	**14**
Total Risk Score *(Rel x likelihood):*	**14**

Risk Mitigation	**R9 – Spoofing LiDAR**							
Choose action to take.	Accept:		Defer:		Mitigate:	x	Transfer:	

For the risk, what actions and controls will be used:

Layer where applied	**Description of control or action**	**Estimated cost**
Perception	Multiple LiDAR inputs	High
Perception	Random probing	Low
Perception	Shorten pulse period	Low

Allegro – Worksheet 10		**R10 – Code modification**					
Threat	**Business Asset**	system software					
	Business Asset's Value	High – software is responsible for controlling the car					
	Area of Concern	An attacker uses OBD-II scanner to modify the system code causing unwanted changes and potential harm with loss of integrity of system software.					
	Actor *Who would exploit the area of concern or threat?*	An attacker with some previous experience with car diagnostics and coding can use OBD-II scanner to modify the system code.					
	Means *How would the actor do it? What would they do?*	An attacker uses their knowledge and tools to modify code in the system causing unwanted changes and potential harm.					
	Motive *What is the actor's reason for doing it?*	Wants disrupt the AV program to keep drivers' jobs.					
	Outcome (choose one) *What would be the resulting effect be?*	Disclosure:		Destruction:			
		Modification:	x	Interruption:			
	Security Requirements *How would the information asset's security requirements be breached?*	System software can be modified, no validation.					
	Likelihood (choose one)	High:		Medium:		Low:	x

Consequences *What are the consequences to the organization as a result of the risk?*	**Severity** *How severe are the consequences to the organization or asset owner by impact area?* **3 for highest priority, 2 for medium and 1 for lowest*			
Modifying the code will cause unwanted errors and can possibly be used to harm the car or other road users. Depending on the modified code, it can break the system making it unavailable to use. Using the tools will allow the attacker to see the code used in the system.	Impact area	Priority*	Impact	Score
	Confidentiality	1	Medium	2
	Availability	3	High	9
	Integrity	2	High	6

Relative risk score:	**17**
Total Risk Score *(Rel x likelihood):*	**17**

Risk Mitigation	**R10 – Code modification**						
Choose action to take.	Accept:		Defer:		Mitigate:	x	Transfer:

For the risk, what actions and controls will be used:

Layer where applied	**Description of control or action**	**Estimated cost**
Application	Device authentication	Medium
Application	Anti-malware	Low
Application	Isolation	Medium

Allegro – Worksheet 10		**R11 – Code injection**					
Threat	**Business Asset**	system software					
	Business Asset's Value	High – software is responsible for controlling the car					
	Area of Concern	An attacker uses OBD-II scanner to inject code the system code causing unwanted changes and potential harm with loss of integrity of system software.					
	Actor *Who would exploit the area of concern or threat?*	An attacker with some previous experience with car diagnostics and coding can use OBD-II scanner to inject harmful code into the system.					
	Means *How would the actor do it? What would they do?*	An attacker uses their knowledge and tools to inject code in the system causing unwanted changes and potential harm.					
	Motive *What is the actor's reason for doing it?*	Wants disrupt the AV program to keep drivers' jobs.					
	Outcome (choose one) *What would be the resulting effect be?*	Disclosure:		Destruction:			
		Modification:	x	Interruption:			
	Security Requirements *How would the information asset's security requirements be breached?*	Harmful code can be injected into system software, no validation.					
	Likelihood (choose one)	High:		Medium:		Low:	x

Consequences *What are the consequences to the organization as a result of the risk?*	**Severity** *How severe are the consequences to the organization or asset owner by impact area?* **3 for highest priority, 2 for medium and 1 for lowest*			
Injecting any kind of harmful code into the system will cause impacts to confidentiality, integrity and availability. The code could collect confidential data, shut down parts of the system, cause wrong decisions in the controlling of the cars. All this impacts the business, but can also harm other road users when the car is on the move.	Impact area	Priority*	Impact	Score
	Confidentiality	1	High	3
	Availability	2	High	6
	Integrity	3	High	9

Relative risk score:	**18**
Total Risk Score *(Rel x likelihood):*	**18**

Risk Mitigation	**R11 – Code injection**						
Choose action to take.	Accept:		Defer:		Mitigate:	x	Transfer:
For the risk, what actions and controls will be used:							

Layer where applied	**Description of control or action**	**Estimated cost**
Application	Device authentication	Medium
Application	Anti-malware	Low
Application	Isolation	Medium

Allegro – Worksheet 10		**R12 – Packet sniffing**
Threat	**Business Asset**	Communication data
	Business Asset’s Value	High - without communication the components can’t work together
	Area of Concern	An attacker uses packet sniffer to intercept and collect data from communications in the system causing loss of confidentiality in the communication data.
	Actor *Who would exploit the area of concern or threat?*	An attacker with a packet sniffer and some previous experience.
	Means *How would the actor do it? What would they do?*	An attacker uses packet sniffer to intercept and collect data from communications in the system.
	Motive *What is the actor’s reason for doing it?*	Wants to gather classified data to sell to competitors.
	Outcome (choose one) *What would be the resulting effect be?*	Disclosure: x Destruction: Modification: Interruption:
	Security Requirements *How would the information asset’s security requirements be breached?*	Communication can be intercepted.
	Likelihood (choose one)	High: Medium: x Low:

Consequences *What are the consequences to the organization as a result of the risk?*	**Severity** *How severe are the consequences to the organization or asset owner by impact area?* **3 for highest priority, 2 for medium and 1 for lowest*			
The packet sniffer can gather data without any interruptions in a system with no detection or mitigation. The data communicated in the system can be confidential and harmful in wrong hands. Correctly installed sniffer won’t cause any interruptions in the communications and availability is not affected. Packet sniffing does not affect the integrity of the communication (data will still be the same as the original).	Impact area	Priority*	Impact	Score
	Confidentiality	3	High	9
	Availability	1	Low	1
	Integrity	2	Low	2

Relative risk score:	**12**
Total Risk Score *(Rel x likelihood):*	**24**

Risk Mitigation	**R12 – Packet sniffing**						
Choose action to take.	Accept:		Defer:		Mitigate:	x	Transfer:

For the risk, what actions and controls will be used:

Layer where applied	**Description of control or action**	**Estimated cost**
Network	Encryption	Medium
Network	Device authentication	Medium
Network	User authentication	Medium

Allegro – Worksheet 10		**R13 – Packet fuzzing**					
Threat	**Business Asset**	Communication data					
	Business Asset's Value	High - without communication the components can't work together					
	Area of Concern	An attacker sends invalid data to the system causing unwanted errors and potentially exposing loopholes in the security causing loss of integrity in the communication data.					
	Actor *Who would exploit the area of concern or threat?*	An attacker with some experience working with data packages.					
	Means *How would the actor do it? What would they do?*	An attacker uses their experience to send invalid data to the system causing unwanted errors and potentially exposing security loopholes					
	Motive *What is the actor's reason for doing it?*	Wants to find loopholes and cause errors in the vehicle.					
	Outcome (choose one) *What would be the resulting effect be?*	Disclosure:		Destruction:			
		Modification:	x	Interruption:			
	Security Requirements *How would the information asset's security requirements be breached?*	System can't handle invalid data inputs.					
	Likelihood (choose one)	High:		Medium:		Low:	x

Consequences *What are the consequences to the organization as a result of the risk?*	**Severity** *How severe are the consequences to the organization or asset owner by impact area?* **3 for highest priority, 2 for medium and 1 for lowest*			
Without any input validation, tempering with communication data will cause errors in the system. The outcomes could be used to find loopholes in the security for other attacks or just manipulating the vehicle to attackers control.	Impact area	Priority*	Impact	Score
	Confidentiality	3	High	9
	Availability	1	Medium	2
	Integrity	2	Medium	4
		Relative risk score:		**15**
		Total Risk Score *(Rel x likelihood):*		**15**

Risk Mitigation	**R13 – Packet fuzzing**						
Choose action to take.	Accept:		Defer:		Mitigate:	x	Transfer:
For the risk, what actions and controls will be used:							

Layer where applied	**Description of control or action**	**Estimated cost**
Network	Encryption	High
Network	Device authentication	Medium
Network	User authentication	Medium

Allegro – Worksheet 10		**R14 –Eavesdropping CAN**					
Threat	**Business Asset**	Communication data					
	Business Asset's Value	High - without communication the components can't work together					
	Area of Concern	An attacker uses their tools and motivation to listen to CAN bus, gaining access to communication data and causing the loss of confidentiality of communication data					
	Actor *Who would exploit the area of concern or threat?*	An attacker with tools and motivation to listen to CAN bus messages					
	Means *How would the actor do it? What would they do?*	An attacker uses their tools and motivation to listen to CAN bus gaining access to communication data					
	Motive *What is the actor's reason for doing it?*	Wants to gather classified data to sell to competitors.					
	Outcome (choose one) *What would be the resulting effect be?*	Disclosure:	x	Destruction:			
		Modification:		Interruption:			
	Security Requirements *How would the information asset's security requirements be breached?*	CAN bus can be listened to by outsiders					
	Likelihood (choose one)	High:		Medium:		Low:	x

Consequences *What are the consequences to the organization as a result of the risk?*	**Severity** *How severe are the consequences to the organization or asset owner by impact area?* **3 for highest priority, 2 for medium and 1 for lowest*			
Listening to CAN messages can reveal confidential information to outsiders. The impact will be less (but still high) than listening to the full communication as CAN is only one channel of many different ones. Correctly installed sniffer won't cause any interruptions in the communications and availability is not affected nor is the integrity as the messages should not be modified to avoid finding out.	Impact area	Priority*	Impact	Score
	Confidentiality	3	High	9
	Availability	1	Low	1
	Integrity	2	Low	2
		Relative risk score:		**12**
		Total Risk Score *(Rel x likelihood):*		**12**

Risk Mitigation	**R14 –Eavesdropping CAN**							
Choose action to take.	Accept:		Defer:		Mitigate:	x	Transfer:	
For the risk, what actions and controls will be used:								

Layer where applied	**Description of control or action**	**Estimated cost**
Network	Encryption	High
Network	Device authentication	Medium
Network	User authentication	Medium

Allegro – Worksheet 10		**R15– Inject CAN messages**					
Threat	**Business Asset**	Communication data					
	Business Asset's Value	High - without communication the components can't work together					
	Area of Concern	An attacker uses their tools to inject CAN messages causing disturbances in the system and possible accidents and causing the loss of integrity of communication data.					
	Actor *Who would exploit the area of concern or threat?*	An attacker with tools to inject CAN messages.					
	Means *How would the actor do it? What would they do?*	An attacker uses their tools to inject CAN messages causing disturbances in the system and possible accidents.					
	Motive *What is the actor's reason for doing it?*	Wants disrupt the AV program to keep drivers' jobs.					
	Outcome (choose one) *What would be the resulting effect be?*	Disclosure:	x	Destruction:			
		Modification:		Interruption:			
	Security Requirements *How would the information asset's security requirements be breached?*	No authentication for CAN messages.					
	Likelihood (choose one)	High:		Medium:		Low:	x

Consequences *What are the consequences to the organization as a result of the risk?*	**Severity** *How severe are the consequences to the organization or asset owner by impact area?* **3 for highest priority, 2 for medium and 1 for lowest*			
Injecting CAN messages will cause errors in the system and possible accidents. Invalid messages cause wrong decisions by driving planner and harm to the vehicle or passengers is possible. The messages can be used to shut down important components.	Impact area	Priority*	Impact	Score
	Confidentiality	2	Medium	4
	Availability	1	Medium	2
	Integrity	3	High	9
		Relative risk score:		**15**
		Total Risk Score *(Rel x likelihood):*		**15**

Risk Mitigation	**R15– Inject CAN messages**							
Choose action to take.	Accept:		Defer:		Mitigate:	x	Transfer:	
For the risk, what actions and controls will be used:								

Layer where applied	**Description of control or action**	**Estimated cost**
Network	Encryption	High
Network	Device authentication	Medium
Network	User authentication	Medium

Allegro – Worksheet 10		**R16 – GPS jamming and spoofing**					
Threat	**Business Asset**	Location data					
	Business Asset's Value	High – Knowing the location is essential for AV					
	Area of Concern	An attacker can use their tools to send modified signals to jam the GPS, making the vehicle localization not possible and causing the loss of integrity of location data					
	Actor *Who would exploit the area of concern or threat?*	An attacker with tools to send GPS signals.					
	Means *How would the actor do it? What would they do?*	An attacker can use their tools to send modified signals to jam the GPS, making the vehicle localization not possible.					
	Motive *What is the actor's reason for doing it?*	Wants disrupt the AV program to keep drivers' jobs.					
	Outcome (choose one) *What would be the resulting effect be?*	Disclosure:		Destruction:			
		Modification:		Interruption:	x		
	Security Requirements *How would the information asset's security requirements be breached?*	GPS in not jamming resistant.					
	Likelihood (choose one)	High:		Medium:	x	Low:	

Consequences *What are the consequences to the organization as a result of the risk?*	**Severity** *How severe are the consequences to the organization or asset owner by impact area?* **3 for highest priority, 2 for medium and 1 for lowest*			
Losing the integrity of data will cause the system to make wrong decisions and potential harm to other road users. Not having the sensor available without any mitigations will cause the system to not see the outside, possibly other sensors can cover. Jamming GPS sensor will not cause any data leaks.	Impact area	Priority*	Impact	Score
	Confidentiality	1	Low	1
	Availability	3	High	9
	Integrity	2	High	6

Relative risk score:	**16**
Total Risk Score *(Rel x likelihood):*	**32**

Risk Mitigation	**R16 – GPS jamming**						
Choose action to take.	Accept:		Defer:		Mitigate:	x	Transfer:
For the risk, what actions and controls will be used:							

Layer where applied	**Description of control or action**	**Estimated cost**
Perception	Nullification	High
Perception	Monitoring signals and identification nodes	Medium

Allegro – Worksheet 10		**R17 – EMP attacks**					
Threat	**Business Asset**	Autonomous driving					
	Business Asset's Value	High – Without autonomous driving, it is a normal car					
	Area of Concern	An attacker uses EMP generator to shut down components in the AV, making autonomous driving impossible and causing the loss of availability of autonomous driving					
	Actor *Who would exploit the area of concern or threat?*	An attacker with EMP generator.					
	Means *How would the actor do it? What would they do?*	An attacker uses EMP generator to shut down components in the AV, making autonomous driving impossible.					
	Motive *What is the actor's reason for doing it?*	Wants disrupt the AV program to keep drivers' jobs.					
	Outcome (choose one) *What would be the resulting effect be?*	Disclosure:		Destruction:			
		Modification:		Interruption:	x		
	Security Requirements *How would the information asset's security requirements be breached?*	Electronic components in AV can be affected with EMP.					
	Likelihood (choose one)	High:		Medium:		Low:	x

Consequences *What are the consequences to the organization as a result of the risk?*	**Severity** *How severe are the consequences to the organization or asset owner by impact area?* **3 for highest priority, 2 for medium and 1 for lowest*			
EMP attacks can shut down components in the car. Depending on the pulse generated, the impact is different. Small pulse may only affect very small components but bigger ones can affect larger components and even cause permanent damage. Generating high impact pulses is hard and the tools used are expensive.	Impact area	Priority*	Impact	Score
	Confidentiality	1	Low	1
	Availability	3	High	9
	Integrity	2	Low	2

Relative risk score:	**12**
Total Risk Score *(Rel x likelihood):*	**12**

Risk Mitigation	**R17 – EMP attacks**						
Choose action to take.	Accept:		Defer:		Mitigate:	x	Transfer:

For the risk, what actions and controls will be used:

Layer where applied	**Description of control or action**	**Estimated cost**
All	Isolation	Medium

Allegro – Worksheet 10		**R18 – Inject malware**					
Threat	**Business Asset**	Autonomous driving					
	Business Asset's Value	High – Without autonomous driving, it is a normal car					
	Area of Concern	An attacker uses physical ports or network to inject malware into the system, causing errors, loss of data, accidents and loss of integrity of autonomous driving.					
	Actor *Who would exploit the area of concern or threat?*	An attacker with access to ports or network to inject malware.					
	Means *How would the actor do it? What would they do?*	An attacker uses physical ports or network to inject malware into the system.					
	Motive *What is the actor's reason for doing it?*	Depending on the malware, the attacker can gather classified data, disturb the processes and so on.					
	Outcome (choose one) *What would be the resulting effect be?*	Disclosure:		Destruction:	x		
		Modification:		Interruption:			
	Security Requirements *How would the information asset's security requirements be breached?*	Physical port or network can be used to inject malware.					
	Likelihood (choose one)	High:		Medium:	x	Low:	

Consequences *What are the consequences to the organization as a result of the risk?*	**Severity** *How severe are the consequences to the organization or asset owner by impact area?* **3 for highest priority, 2 for medium and 1 for lowest*			
Having malware in the system can cause a lot of trouble. Having affected the system, it will be easier to add more malware. All of this can have the attacker gather data, disturb the driving process, causing harm to the components and so on. Overall outcome is the destruction of the autonomous driving process.	Impact area	Priority*	Impact	Score
	Confidentiality	3	High	9
	Availability	2	High	6
	Integrity	1	High	3

Relative risk score:	**18**
Total Risk Score *(Rel x likelihood):*	**36**

Risk Mitigation	**R18 – Inject malware**						
Choose action to take.	Accept:		Defer:		Mitigate:	x	Transfer:
For the risk, what actions and controls will be used:							

Layer where applied	**Description of control or action**	**Estimated cost**
Application, Network	Install firewall	Low
Application	Anti-malware	Low
Application	Isolation	Medium

Allegro – Worksheet 10		**R19 – Manipulate map data**					
Threat	**Business Asset**	Map data					
	Business Asset’s Value	High – Map is required to know where roads are					
	Area of Concern	An attacker uses their access to the maps to manipulate them, resulting in traffic disturbances and accidents and loss of integrity of map data.					
	Actor *Who would exploit the area of concern or threat?*	An attacker with access to the storage and maps.					
	Means *How would the actor do it? What would they do?*	An attacker uses their access to the maps to manipulate them, resulting in traffic disturbances and accidents.					
	Motive *What is the actor’s reason for doing it?*	Wants disrupt the AV program to keep drivers’ jobs.					
	Outcome (choose one) *What would be the resulting effect be?*	Disclosure:		Destruction:			
		Modification:	x	Interruption:			
	Security Requirements *How would the information asset’s security requirements be breached?*	Storage and map data are not authenticated.					
	Likelihood (choose one)	High:		Medium:		Low:	x

Consequences *What are the consequences to the organization as a result of the risk?*	**Severity** *How severe are the consequences to the organization or asset owner by impact area?* **3 for highest priority, 2 for medium and 1 for lowest*			
Map data is crucial for the vehicle to know where and how it should drive. Manipulating the lines used to locate the car on the street could make the car drive on sideways or even hit objects.	Impact area	Priority*	Impact	Score
	Confidentiality	2	Low	2
	Availability	1	Low	1
	Integrity	3	High	9

Relative risk score:	**12**
Total Risk Score *(Rel x likelihood):*	**12**

Risk Mitigation	**R19 – Manipulate map data**							
Choose action to take.	Accept:		Defer:		Mitigate:	x	Transfer:	

For the risk, what actions and controls will be used:		
Layer where applied	**Description of control or action**	**Estimated cost**
Application	Isolation	Medium
Application	Device authentication	Medium
Application	User authentication	Medium

Allegro – Worksheet 10		**R20 – Extract map data**					
Threat	**Business Asset**	Map data					
	Business Asset's Value	High – Map is required to know where roads are					
	Area of Concern	An attacker uses their access to the maps to manipulate them, resulting in information leak and loss of confidentiality of map data.					
	Actor *Who would exploit the area of concern or threat?*	An attacker with access to the storage and maps.					
	Means *How would the actor do it? What would they do?*	An attacker uses their access to the maps to extract them, causing information leak.					
	Motive *What is the actor's reason for doing it?*	Wants disrupt the AV program to keep drivers' jobs.					
	Outcome (choose one) *What would be the resulting effect be?*	Disclosure:	x	Destruction:			
		Modification:		Interruption:			
	Security Requirements *How would the information asset's security requirements be breached?*	Storage and map data are not authenticated.					
	Likelihood (choose one)	High:		Medium:		Low:	x

Consequences *What are the consequences to the organization as a result of the risk?*	**Severity** *How severe are the consequences to the organization or asset owner by impact area?* **3 for highest priority, 2 for medium and 1 for lowest*			
Gaining access to the map data will cause potential risks in other aspects. Knowing what lines and what streets will most likely be used can be used by the attacker to prepare other attacks. Selling of the data is possible.	Impact area	Priority*	Impact	Score
	Confidentiality	3	High	9
	Availability	1	Low	1
	Integrity	2	Low	2
		Relative risk score:		**12**
		Total Risk Score *(Rel x likelihood):*		**12**

Risk Mitigation	**R20 – Extract map data**						
Choose action to take.	Accept:		Defer:		Mitigate:	x	Transfer:
For the risk, what actions and controls will be used:							

Layer where applied	**Description of control or action**	**Estimated cost**
Application	Isolation	Medium
Application	Device authentication	Medium
Application	User authentication	Medium

Allegro – Worksheet 10		**R21 – Delete map data**
Threat	**Business Asset**	Map data
	Business Asset's Value	High – Map is required to know where roads are
	Area of Concern	An attacker uses their access to the maps to delete them, resulting in traffic disturbances and accidents and loss of availability of map data.
	Actor *Who would exploit the area of concern or threat?*	An attacker with access to the storage and maps.
	Means *How would the actor do it? What would they do?*	An attacker uses their access to the maps to delete them, resulting in traffic disturbances and accidents.
	Motive *What is the actor's reason for doing it?*	Wants disrupt the AV program to keep drivers' jobs.

Outcome (choose one) *What would be the resulting effect be?*	Disclosure:		Destruction:	x
	Modification:		Interruption:	

Security Requirements *How would the information asset's security requirements be breached?*	Storage and map data are not authenticated.

Likelihood (choose one)	High:		Medium:		Low:	x

Consequences *What are the consequences to the organization as a result of the risk?*	**Severity** *How severe are the consequences to the organization or asset owner by impact area?* **3 for highest priority, 2 for medium and 1 for lowest*			
Map data is crucial for autonomous driving. Destroying it will cause the vehicle to stop and continuing the work is impossible until new data is provided.	Impact area	Priority*	Impact	Score
	Confidentiality	2	Low	2
	Availability	3	High	9
	Integrity	1	Low	1

Relative risk score:	**12**
Total Risk Score *(Rel x likelihood):*	**12**

Risk Mitigation	**R21 – Delete map data**						
Choose action to take.	Accept:		Defer:		Mitigate:	x	Transfer:

For the risk, what actions and controls will be used:

Layer where applied	**Description of control or action**	**Estimated cost**
Application	Isolation	Medium
Application	Device authentication	Medium
Application	User authentication	Medium

Allegro – Worksheet 10		**R22 – Disable actuation module**					
Threat	**Business Asset**	Autonomous driving					
	Business Asset’s Value	High – Without autonomous driving, it is a normal car					
	Area of Concern	An attacker installs malware on the actuation module, which can disable the functions of it causing loss of availability of autonomous driving					
	Actor *Who would exploit the area of concern or threat?*	An attacker who can install malware on the actuation module.					
	Means *How would the actor do it? What would they do?*	An attacker installs malware on the actuation module, which can disable the functions of it.					
	Motive *What is the actor’s reason for doing it?*	Wants disrupt the AV program to keep drivers’ jobs.					
	Outcome (choose one) *What would be the resulting effect be?*	Disclosure:			Destruction:		
		Modification:			Interruption:	x	
	Security Requirements *How would the information asset’s security requirements be breached?*	Actuation module is not theft proof.					
	Likelihood (choose one)	High:		Medium:		Low:	x

Consequences *What are the consequences to the organization as a result of the risk?*	**Severity** *How severe are the consequences to the organization or asset owner by impact area?* **3 for highest priority, 2 for medium and 1 for lowest*			
Actuation module is responsible to carry out the controls given by computing unit. Without it, autonomous driving is impossible. Disabling the actuation module can be used to demand money for the malware removal.	Impact area	Priority*	Impact	Score
	Confidentiality	1	Low	1
	Availability	3	High	9
	Integrity	2	Medium	4
	Relative risk score:			**14**
	Total Risk Score *(Rel x likelihood):*			**14**

Risk Mitigation	**R22 – Disable actuation module**						
Choose action to take.	Accept:		Defer:		Mitigate:	x	Transfer:

For the risk, what actions and controls will be used:		
Layer where applied	**Description of control or action**	**Estimated cost**
Application	Isolation	Medium
Application	Access Control	Low

Allegro – Worksheet 10		**R23 – Induce bad analysis**
Threat	**Business Asset**	Autonomous driving
	Business Asset's Value	High – Without autonomous driving, it is a normal car
	Area of Concern	An attacker uses their knowledge to create fake output of the software causing the car to follow attackers orders and causing loss of integrity of decision maker and driving planner
	Actor *Who would exploit the area of concern or threat?*	An attacker with knowledge on the used software.
	Means *How would the actor do it? What would they do?*	An attacker uses their knowledge to create fake output of the software causing the car to follow attackers orders.
	Motive *What is the actor's reason for doing it?*	Wants disrupt the AV program to keep drivers' jobs.

Outcome (choose one) *What would be the resulting effect be?*	Disclosure:		Destruction:	
	Modification:	x	Interruption:	

Security Requirements *How would the information asset's security requirements be breached?*	Software in computing unit is not protected.

Likelihood (choose one)	High:		Medium:		Low:	x

Consequences *What are the consequences to the organization as a result of the risk?*	**Severity** *How severe are the consequences to the organization or asset owner by impact area?* **3 for highest priority, 2 for medium and 1 for lowest*			
Inducing bad analysis makes the vehicle to be controlled by the attacker. The attacker can choose what inputs will be given to the actuation module, as they know what the inputs are and how they would be used. Letting an attacker control the car can cause harm to the car itself, passengers or other road users and their property.	Impact area	Priority*	Impact	Score
	Confidentiality	1	Low	1
	Availability	2	Medium	4
	Integrity	3	High	9

Relative risk score:	**14**
Total Risk Score *(Rel x likelihood):*	**14**

Risk Mitigation	**R23 – Induce bad analysis**						
Choose action to take.	Accept:		Defer:		Mitigate:	x	Transfer:

For the risk, what actions and controls will be used:

Layer where applied	**Description of control or action**	**Estimated cost**
Application	Isolation	Medium
Application	Access Control	Low
Application	Input validation	Low

II. Validated OCTAVE Worksheets

Allegro – Worksheet 10		**R4 – Jamming radar**					
Threat	**Business Asset**	Surrounding environment data					
	Business Asset's Value	***Low – Losing radar data does not impact BOLT AV***					
	Area of Concern	An attacker uses their tools to manipulate the data received by the radar causing false blackout on the radar and loss of integrity of surrounding environment data.					
	Actor *Who would exploit the area of concern or threat?*	An attacker with some previous experience with radars and has signal generator (+multiplier etc.).					
	Means *How would the actor do it? What would they do?*	An attacker uses their knowledge and tools to carry out a jamming attack on radar by emitting frequencies used by the sensors and causing false information (distance constantly changing) received (76-77GHz in the experiment).					
	Motive *What is the actor's reason for doing it?*	Wants disrupt the AV program to keep drivers' jobs.					
	Outcome (choose one) *What would be the resulting effect be?*	Disclosure:		Destruction:			
		Modification:		Interruption:	x		
	Security Requirements *How would the information asset's security requirements be breached?*	Radars are not jamming resistant.					
	Likelihood (choose one)	High:		Medium:	x	Low:	

Consequences *What are the consequences to the organization as a result of the risk?*	**Severity** *How severe are the consequences to the organization or asset owner by impact area?* **3 for highest priority, 2 for medium and 1 for lowest*			
Losing the integrity of data will cause the system to make wrong decisions and potential harm to other road users. Not having the sensor available without any mitigations will cause the system to not see the outside, possibly other sensors can cover. Jamming attack on radar will not cause any data leaks.	Impact area	Priority*	Impact	Score
	Confidentiality	1	Low	1
	Availability	3	High	9
	Integrity	2	High	6

Relative risk score:	**16**
Total Risk Score *(Rel x likelihood):*	**32**

Risk Mitigation	**R4 – Jamming radar**							
Choose action to take.	Accept:		Defer:		Mitigate:	x	Transfer:	

For the risk, what actions and controls will be used:

Layer where applied	**Description of control or action**	**Estimated cost**
Perception	Noise detection and rejection	Low
Perception	Multiple sensors for redundancy check	Low

Allegro – Worksheet 10		**R5 – Spoofing radar**					
Threat	**Business Asset**	Surrounding environment data					
	Business Asset's Value	***Low – Losing radar data does not impact BOLT AV***					
	Area of Concern	An attacker uses their tools to manipulate the data received by the radar causing constant changes in distance/velocity on the radar and loss of integrity of surrounding environment data.					
	Actor *Who would exploit the area of concern or threat?*	An attacker with some previous experience with radars and has signal generator (+multiplier etc.).					
	Means *How would the actor do it? What would they do?*	An attacker uses their knowledge and tools to carry out a spoofing attack on radar by emitting frequencies used by the sensors and causing false information (no objects detected) received (76-77GHz in the experiment)					
	Motive *What is the actor's reason for doing it?*	Wants disrupt the AV program to keep drivers' jobs.					
	Outcome (choose one) *What would be the resulting effect be?*	Disclosure:		Destruction:			
		Modification:		Interruption:	x		
	Security Requirements *How would the information asset's security requirements be breached?*	Radars are not spoofing resistant.					
	Likelihood (choose one)	High:		Medium:	x	Low:	

Consequences *What are the consequences to the organization as a result of the risk?*	**Severity** *How severe are the consequences to the organization or asset owner by impact area?* **3 for highest priority, 2 for medium and 1 for lowest*			
Losing the integrity of data will cause the system to make wrong decisions and potential harm to other road users. Not having the radar available without any mitigations will cause the system to not see the outside, possibly other sensors can cover. Spoofing attack on radar will not cause any data leaks.	Impact area	Priority*	Impact	Score
	Confidentiality	1	Low	1
	Availability	2	High	6
	Integrity	3	High	9

Relative risk score:	**16**
Total Risk Score *(Rel x likelihood):*	**32**

Risk Mitigation	**R5 – Spoofing radar**							
Choose action to take.	Accept:		Defer:		Mitigate:	x	Transfer:	
For the risk, what actions and controls will be used:								
Layer where applied	**Description of control or action**						**Estimated cost**	
Perception	Noise detection and rejection						Low	
Perception	Multiple sensors for redundancy check						Low	

Allegro – Worksheet 10		**R7 – Confusing controls with attack on cameras**					
Threat	**Business Asset**	Video and Image data					
	Business Asset's Value	***High – Image recognition is essential for safe driving***					
	Area of Concern	An attacker uses their tools to send malicious optical short output and blind cameras causing unwanted blindness and confusion for longer period, possible hardware damage and loss of integrity of video and image data.					
	Actor *Who would exploit the area of concern or threat?*	An attacker with some previous experience and tools to send malicious optical inputs (laser etc.), tools to further destabilize the input.					
	Means *How would the actor do it? What would they do?*	An attacker uses their knowledge and malicious optical emitters to send a short output and blind cameras causing unwanted blindness, confusion for longer period *and **messing with auto exposure*** on the cameras and possibly permanently damage the camera sensors.					
	Motive *What is the actor's reason for doing it?*	***Mess with image recognition to cause accidents.***					
	Outcome (choose one) *What would be the resulting effect be?*	Disclosure:			Destruction:		
		Modification:			Interruption:		x
	Security Requirements *How would the information asset's security requirements be breached?*	Cameras are vulnerable to blinding attacks.					
	Likelihood (choose one)	***High:***	***x***	Medium:		Low:	

Consequences *What are the consequences to the organization as a result of the risk?*	**Severity** *How severe are the consequences to the organization or asset owner by impact area?* _*3 for highest priority, 2 for medium and 1 for lowest_			
Using lasers to carry out the attack can permanently damage the camera's lens. Messing with camera inputs and auto exposure will make it harder to detect traffic lights, signs and pedestrians. More likely to cause accidents.	Impact area	Priority*	Impact	Score
	Confidentiality	1	Low	1
	Availability	3	High	9
	Integrity	2	High	6
	Relative risk score:			**16**
	Total Risk Score *(Rel x likelihood):*			***48***

Risk Mitigation	**R7 – Confusing controls with attack on cameras**							
Choose action to take.	Accept:		Defer:		Mitigate:	x	Transfer:	

For the risk, what actions and controls will be used:

Layer where applied	**Description of control or action**	**Estimated cost**
Perception	Overlapping image output with multiple cameras	Low
Perception	Turn off auto exposure	Low

Allegro – Worksheet 10		**R8 – Relay attack on LiDAR**
Threat	**Business Asset**	Surrounding environment data
	Business Asset's Value	High – Without Surrounding environment data, car cannot continue
	Area of Concern	An attacker uses their tools to send a light wave and manipulating the information got by the LIDAR to carry out the relay attack causing confusion, errors and loss of integrity of surrounding environment data. ***Manipulating with the LiDAR inputs could possibly be used to control the car.***
	Actor *Who would exploit the area of concern or threat?*	An attacker with some previous experience and tools to send light with specific (905nm) wavelengths, oscilloscope.
	Means *How would the actor do it? What would they do?*	An attacker uses their knowledge and tools to carry out a relay attack confusing and manipulating the data received by the LIDAR causing unwanted errors.
	Motive *What is the actor's reason for doing it?*	Wants disrupt the AV program to keep drivers' jobs.
	Outcome (choose one) *What would be the resulting effect be?*	Disclosure: ⬚ Destruction: ⬚ Modification: x Interruption:
	Security Requirements *How would the information asset's security requirements be breached?*	LIDAR's are not relay attack resistant.
	Likelihood (choose one)	High: Medium: Low: x

Disclosure:		Destruction:	
Modification:	x	Interruption:	

Likelihood (choose one)	High:		Medium:		Low:	x

Consequences *What are the consequences to the organization as a result of the risk?*	**Severity** *How severe are the consequences to the organization or asset owner by impact area?* **3 for highest priority, 2 for medium and 1 for lowest*			
Modifying LiDAR inputs in certain way can be used to control the car by an attacker.	Impact area	Priority*	Impact	Score
	Confidentiality	1	Low	1
	Availability	3	High	6
	Integrity	3	High	9
			Relative risk score:	**16**
			Total Risk Score *(Rel x likelihood):*	**16**

Risk Mitigation	**R8 – Relay attack on LiDAR**							
Choose action to take.	Accept:		Defer:		Mitigate:	x	Transfer:	

For the risk, what actions and controls will be used:

Layer where applied	**Description of control or action**	**Estimated cost**
Perception	Multiple LiDAR inputs	High

Allegro – Worksheet 10		**R9 – Spoofing LiDAR**					
Threat	**Business Asset**	surrounding environment data					
	Business Asset's Value	***High – LiDAR is primary tool for obstacle detection***					
	Area of Concern	An attacker uses their knowledge and tools to create objects for LIDAR in the environment, that are not there and causing loss of integrity of surrounding environment data.					
	Actor *Who would exploit the area of concern or threat?*	An attacker with some previous experience and tools to send light with specific (905nm) wavelengths, oscilloscope. ***Create smoke to cause false detections.***					
	Means *How would the actor do it? What would they do?*	An attacker uses their knowledge and tools to create objects for LIDAR in the environment, that are not there.					
	Motive *What is the actor's reason for doing it?*	Wants disrupt the AV program to keep drivers' jobs.					
	Outcome (choose one) *What would be the resulting effect be?*	Disclosure:		Destruction:			
		Modification:		Interruption:	x		
	Security Requirements *How would the information asset's security requirements be breached?*	LIDAR's are not spoofing resistant.					
	Likelihood (choose one)	***High:***	*x*	Medium:		Low:	

Consequences *What are the consequences to the organization as a result of the risk?*	**Severity** *How severe are the consequences to the organization or asset owner by impact area?* **3 for highest priority, 2 for medium and 1 for lowest*			
Creating smoke clouds will cause the LiDAR to detect them as obstacles. Detecting such smoke with LiDAR can cause emergency braking and possible accidents because of that.	Impact area	Priority*	Impact	Score
	Confidentiality	1	Low	1
	Availability	2	Medium	4
	Integrity	3	High	9
	Relative risk score:			**14**
	Total Risk Score *(Rel x likelihood):*			***42***

Risk Mitigation	**R9 – Spoofing LiDAR**							
Choose action to take.	Accept:		Defer:		Mitigate:	x	Transfer:	
For the risk, what actions and controls will be used:								

Layer where applied	**Description of control or action**	**Estimated cost**
Perception	Multiple LiDAR inputs	High
Perception	Better obstacle detection algorithms	Low

Allegro – Worksheet 10		**R10 – Code modification**					
Threat	**Business Asset**	System software					
	Business Asset's Value	High – software is responsible for controlling the car					
	Area of Concern	An attacker uses OBD-II scanner to modify the system code causing unwanted changes and potential harm with loss of integrity of system software. ***Code modification in repositories.***					
	Actor *Who would exploit the area of concern or threat?*	An attacker with some previous experience with car diagnostics and coding can use OBD-II scanner to modify the system code. ***Access to repository to change code.***					
	Means *How would the actor do it? What would they do?*	An attacker uses their knowledge and tools to modify code in the system causing unwanted changes and potential harm.					
	Motive *What is the actor's reason for doing it?*	Wants disrupt the AV program to keep drivers' jobs.					
	Outcome (choose one) *What would be the resulting effect be?*	Disclosure:		Destruction:			
		Modification:	x	Interruption:			
	Security Requirements *How would the information asset's security requirements be breached?*	System software can be modified, no validation.					
	Likelihood (choose one)	High:		Medium:		Low:	x

Consequences *What are the consequences to the organization as a result of the risk?*	**Severity** *How severe are the consequences to the organization or asset owner by impact area?* **3 for highest priority, 2 for medium and 1 for lowest*			
Changing the code in the repository will cause problems with all the cars using the same code. Attacker can use the modified code to cause harm to the next person in the car.	Impact area	Priority*	Impact	Score
	Confidentiality	1	Medium	2
	Availability	3	High	9
	Integrity	2	High	6
	Relative risk score:			**17**
	Total Risk Score *(Rel x likelihood):*			**17**

Risk Mitigation	**R10 – Code modification**						
Choose action to take.	Accept:		Defer:		Mitigate:	x	Transfer:
For the risk, what actions and controls will be used:							

Layer where applied	**Description of control or action**	**Estimated cost**
Application	Unit tests	Low
Application	Regular manual checks	Low
Application	Access control	Low

Allegro – Worksheet 10		**R13 – Packet fuzzing**					
Threat	**Business Asset**	Communication data					
	Business Asset's Value	***High - without communication the components can't work together***					
	Area of Concern	An attacker sends invalid data to the system causing unwanted errors and potentially exposing loopholes in the security causing loss of integrity in the communication data.					
	Actor *Who would exploit the area of concern or threat?*	An attacker with some experience working with data packages.					
	Means *How would the actor do it? What would they do?*	An attacker uses their experience to send invalid data to the system causing unwanted errors and potentially exposing security loopholes					
	Motive *What is the actor's reason for doing it?*	Wants to find loopholes and cause errors in the vehicle.					
	Outcome (choose one) *What would be the resulting effect be?*	Disclosure:		Destruction:			
		Modification:	x	Interruption:			
	Security Requirements *How would the information asset's security requirements be breached?*	System can't handle invalid data inputs.					
	Likelihood (choose one)	High:		Medium:		Low:	x

Consequences *What are the consequences to the organization as a result of the risk?*	**Severity** *How severe are the consequences to the organization or asset owner by impact area?* *3 for highest priority, 2 for medium and 1 for lowest			
Without any input validation, tempering with communication data will cause errors in the system. The outcomes could be used to find loopholes in the security for other attacks or just manipulating the vehicle to attackers control.	Impact area	Priority*	Impact	Score
	Confidentiality	3	High	9
	Availability	1	Medium	2
	Integrity	2	Medium	4
	Relative risk score:			**15**
	Total Risk Score *(Rel x likelihood):*			**15**

Risk Mitigation	**R13 – Packet fuzzing**							
Choose action to take.	Accept:		Defer:		Mitigate:	x	Transfer:	

For the risk, what actions and controls will be used:

Layer where applied	**Description of control or action**	**Estimated cost**
Network	Encryption	High
Network	User authentication	Medium
Network	Secure connection	Medium
Network	Split network (multiple smaller parts)	Low

Allegro – Worksheet 10		**R16 – GPS jamming**					
Threat	**Business Asset**	Location data					
	Business Asset's Value	High – Knowing the location is essential for AV					
	Area of Concern	An attacker can use their tools to send modified signals to jam the GPS, making the vehicle localization not possible and causing the loss of integrity of location data. ***GPS also uses correction got in real-time which could be an attack opportunity.***					
	Actor *Who would exploit the area of concern or threat?*	An attacker with tools to send GPS signals					
	Means *How would the actor do it? What would they do?*	An attacker can use their tools to send modified signals to jam the GPS, making the vehicle localization not possible.					
	Motive *What is the actor's reason for doing it?*	Wants disrupt the AV program to keep drivers' jobs.					
	Outcome (choose one) *What would be the resulting effect be?*	Disclosure:		Destruction:			
		Modification:		Interruption:	x		
	Security Requirements *How would the information asset's security requirements be breached?*	GPS in not jamming resistant.					
	Likelihood (choose one)	High:		Medium:	x	Low:	

Consequences *What are the consequences to the organization as a result of the risk?*	**Severity** *How severe are the consequences to the organization or asset owner by impact area?* **3 for highest priority, 2 for medium and 1 for lowest*			
Losing the integrity of data will cause the system to make wrong decisions and potential harm to other road users. ***The correction is used to get even less error (from meters to few centimetres), messing with it can cause accidents on the road.***	Impact area	Priority*	Impact	Score
	Confidentiality	1	Low	1
	Availability	3	High	9
	Integrity	2	High	6
	Relative risk score:			**16**
	Total Risk Score *(Rel x likelihood):*			**32**

Risk Mitigation	**R16 – GPS jamming**							
Choose action to take.	Accept:		Defer:		Mitigate:	x	Transfer:	
For the risk, what actions and controls will be used:								

Layer where applied	**Description of control or action**	**Estimated cost**
Perception	Duplicate GPS	Medium
Perception	Use LiDAR for localization	Low

<table>
<tr><td colspan="2"><b>Allegro – Worksheet 10</b></td><td colspan="6"><b>R17 – EMP attacks</b></td></tr>
<tr><td rowspan="10"><b>Threat</b></td><td><b>Business Asset</b></td><td colspan="6">Autonomous driving</td></tr>
<tr><td><b>Business Asset’s Value</b></td><td colspan="6">High – Without autonomous driving, it is a normal car</td></tr>
<tr><td><b>Area of Concern</b></td><td colspan="6">An attacker uses EMP generator to shut down components in the AV, making autonomous driving impossible and causing the loss of availability of autonomous driving.</td></tr>
<tr><td><b>Actor</b>
<i>Who would exploit the area of concern or threat?</i></td><td colspan="6">An attacker with EMP generator.</td></tr>
<tr><td><b>Means</b>
<i>How would the actor do it? What would they do?</i></td><td colspan="6">An attacker uses EMP generator to shut down components in the AV, making autonomous driving impossible.</td></tr>
<tr><td><b>Motive</b>
<i>What is the actor’s reason for doing it?</i></td><td colspan="6">Wants disrupt the AV program to keep drivers’ jobs.</td></tr>
<tr><td rowspan="2"><b>Outcome</b> (choose one)
<i>What would be the resulting effect be?</i></td><td colspan="2">Disclosure:</td><td></td><td colspan="2">Destruction:</td><td></td></tr>
<tr><td colspan="2">Modification:</td><td></td><td colspan="2">Interruption:</td><td>x</td></tr>
<tr><td><b>Security Requirements</b>
<i>How would the information asset’s security requirements be breached?</i></td><td colspan="6">Electronic components in AV can be affected with EMP.</td></tr>
<tr><td><b>Likelihood</b> (choose one)</td><td>High:</td><td></td><td>Medium:</td><td></td><td><b><i>Low:</i></b></td><td><b><i>x</i></b></td></tr>
</table>

<table>
<tr><td><b>Consequences</b>
<i>What are the consequences to the organization as a result of the risk?</i></td><td colspan="4"><b>Severity</b>
<i>How severe are the consequences to the organization or asset owner by impact area?</i>
<i>*3 for highest priority, 2 for medium and 1 for lowest</i></td></tr>
<tr><td rowspan="4">EMP attacks can shut down components in the car. Depending on the pulse generated, the impact is different. Small pulse may only affect very small components but bigger ones can affect larger components and even cause permanent damage. Generating high impact pulses is hard and the tools used are expensive.</td><td>Impact area</td><td>Priority*</td><td>Impact</td><td>Score</td></tr>
<tr><td>Confidentiality</td><td>1</td><td>Low</td><td>1</td></tr>
<tr><td>Availability</td><td>3</td><td>High</td><td>9</td></tr>
<tr><td>Integrity</td><td>2</td><td>Low</td><td>2</td></tr>
</table>

Relative risk score:	**12**
Total Risk Score *(Rel x likelihood):*	**12**

<table>
<tr><td><b>Risk Mitigation</b></td><td colspan="8"><b>R17 – EMP attacks</b></td></tr>
<tr><td><b>Choose action to take.</b></td><td><b><i>Accept:</i></b></td><td><i>x</i></td><td>Defer:</td><td></td><td>Mitigate:</td><td></td><td>Transfer:</td><td></td></tr>
<tr><td colspan="9">For the risk, what actions and controls will be used:</td></tr>
<tr><td><b>Layer where applied</b></td><td colspan="5"><b>Description of control or action</b></td><td colspan="3"><b>Estimated cost</b></td></tr>
</table>

Allegro – Worksheet 10		**R19 – Manipulate map data**					
Threat	**Business Asset**	Map data					
	Business Asset's Value	***High – Map is required to know where roads and signs/lights are***					
	Area of Concern	***An attacker uses their access to the maps to manipulate them, resulting in traffic disturbances and accidents and loss of integrity of map data***					
	Actor *Who would exploit the area of concern or threat?*	An attacker with access to the storage and maps. ***Possibly insider***.					
	Means *How would the actor do it? What would they do?*	An attacker uses their access to the maps to manipulate them, resulting in traffic disturbances and accidents.					
	Motive *What is the actor's reason for doing it?*	Wants disrupt the AV program to keep drivers' jobs.					
	Outcome (choose one) *What would be the resulting effect be?*	Disclosure:		Destruction:			
		Modification:	x	Interruption:			
	Security Requirements *How would the information asset's security requirements be breached?*	Storage and map data are not authenticated.					
	Likelihood (choose one)	High:		Medium:		***Low:***	***x***

Consequences *What are the consequences to the organization as a result of the risk?*	**Severity** *How severe are the consequences to the organization or asset owner by impact area?* **3 for highest priority, 2 for medium and 1 for lowest*			
Map data is crucial for the vehicle to know where and how it should drive. Manipulating the lines used to locate the car on the street could make the car drive on sideways or even hit objects.	Impact area	Priority*	Impact	Score
	Confidentiality	2	Low	2
	Availability	1	Low	1
	Integrity	3	High	9
	Relative risk score:			**12**
	Total Risk Score *(Rel x likelihood):*			**12**

Risk Mitigation	**R19 – Manipulate map data**						
Choose action to take.	Accept:		Defer:		Mitigate:	x	Transfer:

For the risk, what actions and controls will be used:

Layer where applied	**Description of control or action**	**Estimated cost**
Application	Duplicated storage (repository, on-board etc.)	Low
Application	Unit tests and simulations on the map	Low