I. Filled OCTAVE Worksheets

Allegi	ro – Worksheet 10	R1	– Jammir	ıg ul	trasonic	sensors		
	Business Asset	Ultr	asonic senso	rs dat	ta			
	Business Asset's Value	Low	v – Losing ul	traso	nic sensors	data does n	ot impact BO	LT AV
	Area of Concern	rece		senso	ors causing	false black	to manipulat out by the ser	
	Actor Who would exploit the area of concern or threat?	An a		some	e previous e		vith ultrasound	d sensors.
+=	Means How would the actor do it? What would they do?	attac	ck on ultraso	nic ra	inging senso	ors by emitti	to carry out a ing frequencie eived by the	s used by
Threat	Motive What is the actor's reason for doing it?		nts disrupt th		program to	keep drive	rs' jobs.	
	Outcome (choose one) What would be the resulting	Ι	Disclosure	:		Destruction:		
	effect be?	Modification:				Interruption:		X
	Security Requirements How would the information asset's security requirements be breached?	Ultr	asonic senso	rs are	e not jammi	ng resistant		
	Likelihood (choose one)	Hig	gh:		Medium:	X	Low:	
What a	equences re the consequences to the organ a result of the risk?	iza-	owner by in	прасі	t area?		e organization	
	the integrity of data will cause the make wrong decisions and poter		Impact area	ı		Priority*	Impact	Score
Not hav	o other road users. ving the sensor available without		Confidentia	ality		1	Low	1
	ions will cause the system to not					2	High	6
Jammir	side, possibly other sensors can co ng attack on ultrasonic sensor will ny data leaks.		Integrity			3	High	9
	•			Rel	lative risl	score:		16
				Tot	tal Risk S	core (Rel :	x likelihood):	32

Risk Mitigation	R1 – Jami	R1 – Jamming ultrasonic sensors										
Choose action to take.	Accept:	Accept: Defer: Mitigate: x Transfer:										
For the risk, what actions and controls will be used:												
Layer where applied	Description	n of c	control or	actio	n	Est	imated cost					
Perception	ception Noise detection and rejection Low											
Perception	Multiple sens	sors fo	r redundancy	check		Low	7					

Allegi	ro – Worksheet 10	R2 -	- S]	poofing	ultrasonic	sensors			
	Business Asset	Ultra	son	ic sensors	data				
	Business Asset's Value	Low	– L	osing ultra	sonic sensors	data does no	ot impact BC	LT AV	
	Area of Concern	mani	pula	ate the da	trasonic freq a received b the sensors a	y the sensor	rs causing fa	lse infor-	
	Actor Who would exploit the area of concern or threat?				me previous o	experience w	vith ultrasoun	d sensors.	
eat	Means How would the actor do it? What would they do?	attacl	k or ienc	n ultrasoni	eir knowledg c ranging ser uences causin	nsors by em	itting careful	ly crafted	
Threat	What is the actor's reason for doing it?								
	Outcome (choose one) What would be the resulting	D)isc	losure:		Destruction:			
	effect be?	Mo	Modification: x			Interr	ruption:		
	Security Requirements How would the information asset's security requirements be breached?	Ultrasonic senso			are not spoof	ing resistant.			
	Likelihood (choose one)	Higl	h:		Medium:	X	Low:		
What a	equences re the consequences to the organ a result of the risk?	niza-	Ho owi	ner by imp	re the conseq act area? priority, 2 fo				
	the integrity of data will cause the make wrong decisions and poter	sys-	_	pact area	1 3	Priority*	Impact	Score	
harm to	o other road users. ving the sensor available without		Coı	nfidentialit	у	1	Low	1	
	ions will cause the system to not					2	High	6	
Spoofin	side, possibly other sensors can co ng attack on ultrasonic sensor will ny data leaks.	ver.		egrity		3	High	9	
	•			F	Relative risk score:				
								32	

Risk Mitigation	R2 – Spoo	R2 – Spoofing ultrasonic sensors										
Choose action to take.	Accept:	Accept: Defer: Mitigate: x Transfer:										
For the risk, what actions and controls will be used:												
Layer where applied	Descriptio	n of c	control or	actio	n	Est	imated cost	t				
Perception	Noise detection and rejection Low											
Perception	Multiple sensors for redundancy check Low											

Business Asset Business Asset's Value Area of Concern 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. An attacker uses their knowledge and materials to cover nearby objects to make them hard to detect by the sensors causing late detection (possible collisions) and loss of integrity of measurement data. An attacker uses their knowledge and materials to cover nearby objects to make them harder to detect with ultrasound sensors. Has sound absorbing materials to use. An attacker uses their knowledge and materials to cover nearby objects to make them harder to detect with ultrasound sensors which causes late detections. Wants disrupt the AV program to keep drivers' jobs. Wants disrupt the AV program to	Allegi	ro – Worksheet 10	R3	– Acoi	ıstic q	uieting			
Area of Concern Area of Concern Actor Who would exploit the area of concern or threat? Means How would the actor do it? What would the actor season for doing it? Outcome (choose one) What would be the resulting effect be? Security Requirements How would the information asset's security requirements be breached? Likelihood (choose one) What are the consequences to the organization as a result of the risk? Consequences What are the consequences to the organization as a result of the risk? Severity Consequences What are the consequences to the organization as a result of the risk? Severity Requirements thou would the information asset's security requirements be breached? Likelihood (choose one) What are the consequences to the organization as a result of the risk? Severity 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 Impact area Priority* Impact Score Confidentiality 1 Low 1 Availability 2 Low 2 Integrity 3 High 9		Business Asset	Ultra	asonic s	ensors d	ata			
make them hard to detect by the sensors causing late detection (possible collisions) and loss of integrity of measurement data. An attacker with some previous experience with ultrasound sensors. Has sound absorbing materials to use. 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 would they do? Outcome (choose one) What would be the resulting effect be? Modification: Disclosure: Destruction: Modification: Interruption: X Consequences What would the information asset's security requirements be breached? Likelihood (choose one) What are the consequences to the organization as a result of the risk? 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 is detected as some objects are hidden. Relative risk score: 12		Business Asset's Value	Low	– Losir	ıg ultras	onic sensors	data does n	ot impact BOI	LT AV
Actor Who would exploit the area of concern or threat? Means How would the actor do it? What would they do? Motive What is the actor's reason for doing it? Outcome (choose one) What would be the resulting effect be? Negurity Requirements How would the information asset's security requirements be breached? Likelihood (choose one) 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: An attacker with some previous experience with ultrasound sensors. Has sound absorbing materials to use. An attacker with some previous experience with ultrasound sensors. Has sound absorbing materials to use. An attacker with some previous experience with ultrasound sensors. Has sound absorbing materials to use. An attacker with some previous experience with ultrasound sensors. Has sound absorbing materials to use. An attacker uses their knowledge and materials to cover nearby objects to make them harder to detect with ultrasound sensors which causes late detections. Wants disrupt the AV program to keep drivers' jobs. Wants disrupt the AV program to keep drivers' jobs. Wants disrupt the AV program to keep drivers' jobs. Watts disrupt the AV program to keep drivers' jobs. Watts disrupt the AV program to keep drivers' jobs. Wants disrupt the AV program to keep drivers' jobs. Watts disrupt the AV program to keep drivers' jobs. Watts disrupt the AV program to keep drivers' jobs. Watts disrupt the AV program to keep drivers' jobs. Watts disrupt the AV program to keep drivers' jobs. Watts disrupt the AV program to keep drivers' jobs. Watts disrupt the AV program to keep drivers' jobs. Watts disrupt the AV program to keep drivers' jobs. Watts disrupt the AV program to keep drivers' jobs. Watts disrupt the AV program to kee		Area of Concern	mak	e them h	ard to d	etect by the	sensors caus	ing late detect	tion (pos-
How would the actor do it? What would they do? Motive What is the actor's reason for doing it? Outcome (choose one) What would be the resulting effect be? Nodification: Security Requirements How would the information asset's security requirements be breached? Likelihood (choose one) What are the consequences to the organization as a result of the risk? 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: Relative risk score: Wants disrupt the AV program to keep drivers' jobs. Wants disrupt the AV program to keep drivers' jobs. Wants disrupt the AV program to keep drivers' jobs. Wants disrupt the AV program to keep drivers' jobs. Wants disrupt the AV program to keep drivers' jobs. Wants disrupt the AV program to keep drivers' jobs. Wants disrupt the AV program to keep drivers' jobs. Wants disrupt the AV program to keep drivers' jobs. Wants disrupt the AV program to keep drivers' jobs. Wants disrupt the AV program to keep drivers' jobs. Wants disrupt the AV program to keep drivers' jobs. Wants disrupt the AV program to keep drivers' jobs. Wants disrupt the AV program to keep drivers' jobs. Wants disrupt the AV program to keep drivers' jobs. Wants disrupt the AV program to keep drivers' jobs. Wants disrupt the AV program to keep drivers' jobs. Wants disrupt the AV program to keep drivers' jobs. Wants disrupt the AV program to keep drivers' jobs. Wants disrupt the AV program to keep drivers' jobs. ### Aution And Interruption: Aution And Interruption: X X X X X X X X X		Who would exploit the area of	An a	ttacker	with son	ne previous	experience w		
Outcome (choose one) What would be the resulting effect be? Modification: Security Requirements How would the information asset's security requirements be breached? Likelihood (choose one) Likelihood (choose one) What are the consequences to the organization as a result of the risk? 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 : Destruction: Modification:	ıt	How would the actor do it?	jects	to mak	e them l	harder to de			
What would be the resulting effect be? Modification: Interruption: x Security Requirements How would the information asset's security requirements be breached? Likelihood (choose one) What would the information asset security requirements be breached? Likelihood (choose one) What would be the resulting Modification: Interruption: x Volume Security Requirements be breached? Likelihood (choose one) What would be the resulting wild research to the information asset on the preached? What would be the resulting wild research to the information asset on the preached? 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 Impact area Priority* Impact Score Confidentiality 1 Low 1 Availability 2 Low 2 Integrity 3 High 9 Relative risk score: 12	Threa	What is the actor's reason for	War	ıts disruj	pt the A	V program t	o keep drive	rs' jobs.	
Security Requirements How would the information asset's security requirements be breached? Likelihood (choose one) Likelihood (choose one) High: Medium: Low: X Consequences What are the consequences to the organization as a result of the risk? 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 is detected as some objects are hidden. Relative risk score: 12		What would be the resulting	I	Disclos	ure:		Destruction:		
How would the information asset's security requirements be breached? Likelihood (choose one) High: Medium: Low: X Consequences What are the consequences to the organization as a result of the risk? 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 i. Relative risk score: 12		effect be?	M	odifica	ation:		Interr	ruption:	X
Consequences What are the consequences to the organization as a result of the risk? 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 i. Relative risk score: 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 Impact area Priority* Impact Score Confidentiality 1 Low 1 Availability 2 Low 2 Integrity 3 High 9		How would the information asset's security requirements	Ultrasonic sensors are not			re not acous	tic quieting 1	resistant.	
What are the consequences to the organization as a result of the risk? 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 . 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 Confidentiality 1 Low 1 Availability 2 Low 2 Integrity 3 High 9 Relative risk score: 12		Likelihood (choose one)	Hig	gh:		Medium		Low:	X
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 . Relative risk score: Confidentiality 1 Low 1 Availability 2 Low 2 Integrity 3 High 9 Relative risk score:	What a tion as	re the consequences to the organ a result of the risk?		How see owner *3 for i	evere ard by impa highest p	ct area?	or medium ar	ıd 1 for lowes	
dents 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 . Relative risk score:	from th	e ultrasonic ranging device. Not	see-	-			Priority*	Impact	Score
cannot be trusted when acoustic quieting is detected as some objects are hidden. No data leaks will be caused by acoustic quieting . Relative risk score: 12	dents a	nd harm to people and other prope	erty.	Confid	entiality		1	Low	1
detected as some objects are hidden. No data leaks will be caused by acoustic quieting . Relative risk score: 112				Availal	oility		2	Low	2
Relative risk score: 12	detected No data	d as some objects are hidden.		Integrit	ty		3	High	9
			Relative risk score:						12

Risk Mitigation	R3 – Acoustic	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										
Perception	Multiple sensors	Multiple sensors for redundancy check Low									

Allegr	ro – Worksheet 10	R4	– Ja	mmin	ıg r	adar			
	Business Asset	Suri	oundi	ing env	iron	ment data			
	Business Asset's Value	High	h – W	ithout S	Surr	ounding env	rironment da	ta, car cannot	continue
	Area of Concern	rada	ır caus	sing fal	se b			e data receiv loss of integr	
	Actor Who would exploit the area of concern or threat?					ne previous iplier etc.).	experience v	vith radars an	d has sig-
at	Means How would the actor do it? What would they do?	attac ing	ck on i false	radar b	y em atio	nitting frequent	encies used b	to carry out a by the sensors nanging) rece	and caus-
Threat	Motive What is the actor's reason for doing it?	War	nts dis	srupt the	e A'		o keep drive		
	Outcome (choose one) What would be the resulting	Disclosure:			:		Destruction:		
	effect be?	M	Modification:		1:		Interr	uption:	X
	Security Requirements How would the information asset's security requirements be breached?	Radars are not ja			mm	ing resistan	t.		
	Likelihood (choose one)	Hig	gh:			Medium:	X	Low:	
What a	equences re the consequences to the organ a result of the risk? the integrity of data will cause the		How own *3 fe	er by in	npac est p	ct area?		e organization ad 1 for lowes Impact	
tem to	make wrong decisions and poter		•				-	•	
Not hav	arm to other road users. Not having the sensor available withou			fidentia			1	Low	1
	nitigations will cause the system to no he outside, possibly other sensors can co			Tivaliaomity			3	High	9
Jammin	amming attack on radar will not cause ata leaks.						2	High	6
1					Relative risk score:				16
				i	Total Risk Score (Rel x likelihood):				32

Risk Mitigation	R4 – Jamming	R4 – Jamming radar									
Choose action to take.	Accept:	Accept: Defer: Mitigate: x Transfer:									
For the risk, what actions and controls will be used:											
Layer where applied	Layer where applied Description of control or action Estimated cost										
Perception	Noise detection and rejection Low										
Perception	Multiple sensors fo	Multiple sensors for redundancy check Low									

Allegr	o – Worksheet 10	R5	- Spoofin	g ra	dar			
	Business Asset	Suri	rounding env	iron	ment data			
	Business Asset's Value	Hig	h – Without	Surro	ounding env	ironment da	ta, car canno	t continue
	Area of Concern	rada		nstar	nt changes ir	distance/ve	ne data receivelocity on the data.	
	Actor Who would exploit the area of concern or threat?	An		som	ne previous e		vith radars an	d has sig-
at	Means How would the actor do it? What would they do?	atta ing	ck on radar b	y em	itting freque	ncies used b	to carry out a by the sensors received (76-	and caus-
Threat	Motive What is the actor's reason for doing it?	Waı	nts disrupt th		program to	keep drive	rs' jobs.	
	Outcome (choose one) What would be the resulting]	Disclosure	•		Destruction:		
	effect be?	M	Iodification	n:		Interr	uption:	X
	Security Requirements How would the information asset's security requirements be breached?	Radars are not spoofing resistant.						
	Likelihood (choose one)	Hig	gh:		Medium:	X	Low:	
What a	equences re the consequences to the organ a result of the risk?	iza-	owner by in	прас	rt area?		e organizatio	
	the integrity of data will cause the make wrong decisions and poten		Impact area	a		Priority*	Impact	Score
Not hav	other road users.		Confidentia	ality		1	Low	1
	ons will cause the system to not		Availability	у		2	High	6
	ide, possibly other sensors can co ag attack on radar will not cause ks.		Integrity			3	High	9
		Relative risk score:					16	
				To	tal Risk S	Score (Rel	x likelihood):	32

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

Allegr	ro – Worksheet 10	R6	– Bli	nding at	tack on c	ameras		
	Business Asset	vide	o and	image data	ì			
	Business Asset's Value		lium – ic ligh		continue dri	ving but car	i't recognize	signs and
	Area of Concern	cam	era cai	using unwa		ess, possible	ous optical d e hardware da	
	Actor Who would exploit the area of concern or threat?				ne previous laser etc.).	experience	and tools to s	end mali-
at	Means How would the actor do it? What would they do?	send	and b	olind came	ras causing		ious optical e indness on th a sensors.	
Threat	Motive What is the actor's reason for doing it?	Wan	ıts disı	rupt the AV	V program t	o keep drive	rs' jobs.	
	Outcome (choose one) What would be the resulting	Ι	Disclo	osure:		Destruction:		
	effect be?	M	odifi	cation:		Interr	ruption:	X
	Security Requirements How would the information asset's security requirements be breached?	Cameras are vulnerable to blinding attacks.						
	Likelihood (choose one)	Hig	gh:	X	Medium:		Low:	
What a	equences re the consequences to the organ a result of the risk?		How owne *3 fo	er by impac r highest p	ct area?	r medium ar	e organizatio	
	g attack will cause some blind sprage recorded by the cameras. B		Impa	ct area		Priority*	Impact	Score
sible ac	an cause not detecting objects and poisons because of that.		Conf	identiality		1	Low	1
	ving the sensor available without		Avai	lability		3	High	9
the outs Using 1	nitigations will cause the system to not ne outside, possibly other sensors can co Using lasers to carry out the attack can			rity		2	High	6
inanent	ly damage the camera's lens	Relative risk score:						16
								48
			Total Risk Score (Rel x likelihood):					

Risk Mitigation	R6 – Blinding	R6 – Blinding attack on cameras										
Choose action to take.	Accept:	Accept: Defer: Mitigate: x Transfer:										
For the risk, what actions and controls will be used:												
Layer where applied	Description of	control or act	tion	Est	imated cost							
Perception Overlapping image output with multiple cameras Low												
Perception	Filter to remove ha	Filter to remove harmful light High										

o – Worksheet 10	R7	Confus	ing o	controls v	vith attacl	k on came	ras	
Business Asset	Vide	eo and Imag	ge dat	a				
Business Asset's Value			can c	ontinue dri	ving but can	't recognize	signs and	
Area of Concern								
					c damage a	110 1055 01 11	neginy of	
Actor					ovnorionoo (and tools to	and mali	
Who would exploit the area of concern or threat?	ciou	s optical inp	outs (l	laser etc.), to	ools to furthe	er destabilize	the input.	
wnai would they ao:						F	-5 F	
Motive	Wan	nts disrupt tl	ne AV	program to	keep drive	rs' jobs.		
What is the actor's reason for doing it?								
_	Ι	Disclosure: Destruction: Modification: Interruption:						
What would be the resulting								
effect be?	M	odificatio	n:		Interr	X		
v <u>-</u>								
Ü	Cam	neras are vul	lnerat	ole to blindi	ng attacks.			
be breached?								
Likelihood (choose one)	Hig	gh:		Medium:	X	Low:		
quences		Severity			•	1		
	iza-				uences to the	e organizatio	on or asset	
a result of the risk?					r modium ar	nd 1 for lowe	c+	
g attack will cause some blind si	oots			110111y, 2 jo			Score	
mage recorded by the cameras. B	lind	1 ······				F ****		
		Confidenti	ality		1	Low	1	
		A !1 . 1. !1!			2	TT' . 1.	0	
			<u>y</u>	-	8	9		
ons will cause the system to not	see	incginy			2	mgn		
	per-							
			Re	lative ris	k score:		16	
						x likelihood):	32	
	Business Asset's Value Area of Concern Actor Who would exploit the area of concern or threat? Means How would the actor do it? What would they do? Motive What is the actor's reason for doing it? Outcome (choose one) What would be the resulting effect be? Security Requirements How would the information asset's security requirements be breached? Likelihood (choose one) quences The the consequences to the organia result of the risk? The gattack will cause some blind in cause not detecting objects and point in the sensor available without ons will cause the system to not ide, possibly other sensors can coiden, possibly other sensors can coiden.	Business Asset Business Asset's Value Area of Concern An and long vide Actor Who would exploit the area of concern or threat? Means How would the actor do it? What would they do? Motive What is the actor's reason for doing it? Outcome (choose one) What would be the resulting effect be? Means How would the information asset's security requirements be breached? Likelihood (choose one) High actor is reason for doing it? Security Requirements How would the information asset's security requirements be breached? Likelihood (choose one) High actor is result of the risk? The security of the risk? The security actor is and posterior in cause not detecting objects and posterior in the sensor available without any one will cause the system to not see ide, possibly other sensors can cover. In sers to carry out the attack can person and contents and cover in sers to carry out the attack can person and contents because of that attack can person and cover in the sensor available without any one will cause the system to not see ide, possibly other sensors can cover. In sers to carry out the attack can person and cover in the sensor actor is the attack can person and cover in the at	Business Asset's Value Business Asset's Value Area of Concern An attacker use and blind came longer period, yideo and image video and image of concern or threat? Means How would the actor do it? What would they do? Motive What is the actor's reason for doing it? Outcome (choose one) What would be the resulting effect be? Modification Security Requirements How would the information asset's security requirements be breached? Likelihood (choose one) Guences The the consequences to the organizative that the consequences the consequences that the consequences that the consequences that	Business Asset Business Asset's Value Area of Concern Actor Who would exploit the area of concern or threat? Means How would the actor do it? What would they do? Motive What is the actor's reason for doing it? Outcome (choose one) What would be the resulting effect be? Modification: Security Requirements How would the information asset's security requirements be breached? Likelihood (choose one) It is consequences to the organizative result of the risk? An attacker uses the and blind cameras concious optical inputs (in the send a short output a and confusion for lonnently damage the cameras and confusion for lonnently damage the cameras for and confusion for lonnently damage the cameras are vulnerated. Cameras are vulnerated by the cameras are vulnerated with the consequences to the organizative result of the risk? Severity How severe are owner by impactive are sult of the risk? Impact area Confidentiality Integrity Regitted the camera's lens. Regitted the came and possible to and possible to the sensor available without any ons will cause the system to not see ide, possibly other sensors can cover. asers to carry out the attack can pery damage the camera's lens.	Business Asset Business Asset's Value Area of Concern Area of Concern Area of Concern Actor Who would exploit the area of concern or threat? Means How would the actor do it? What would they do? An attacker uses their tools to so and blind cameras causing unwavideo and image data. An attacker with some previous cious optical inputs (laser etc.), to an attacker uses their knowledge send a short output and blind camera sensor for doing it? Outcome (choose one) What would be the resulting effect be? Modification: Security Requirements How would the information asset's security requirements be breached? Likelihood (choose one) High: Medium - Car can continue driv traffic lights An attacker uses their knowledge send a short output and blind camently damage the camera sensor wantly damage the camera sensor denerly damage the camera sensor on the first program to the AV	Business Asset Business Asset's Value Area of Concern Area of Concern Area of Concern An attacker uses their tools to send malicio and blind cameras causing unwanted blindr longer period, possible hardware damage a video and image data. An attacker uses their tools to send malicio and blind cameras causing unwanted blindr longer period, possible hardware damage a video and image data. An attacker with some previous experience a cious optical inputs (laser etc.), tools to furthe attack uses their knowledge and malicis send a short output and blind cameras causin and confusion for longer period on the camer nently damage the camera sensors Motive What is the actor's reason for doing it? Outcome (choose one) What would be the resulting effect be? Modification: Destr Modification: Cameras are vulnerable to blinding attacks. be breached? Likelihood (choose one) High: Medium: X Cameras are vulnerable to blinding attacks. be the consequences to the organizative security requirements be breached? Likelihood (choose one) High: Medium: An attacker uses their tools to send malicio and blind cameras causing unwanted blind longer period, possible hardware damage a video and image data. An attacker uses their tools to send malicional bind cameras causing unwanted blind send a short output and blind cameras causing unwanted blind send a short output and blind cameras causing unwanted blind send a short output and blind cameras causing unwanted blinds and confusion for longer period on the camera send a short output and blind cameras causing unwanted blinds and confusion for longer period on the camera sends of the camera sensors Wants disrupt the AV program to keep drive Modification: Interr Security Requirements How would the information asset's security requirements we the consequences to the organizative sensor and position of longer period on the camera sensors How would the information asset's security requirements Wants disrupt the AV program to keep drive Modification: Interr Secur	Business Asset Business Asset's Value Area of Concern Area of Concern Area of Concern Actor Who would exploit the area of concern or threat? Means How would the actor do it? What is the actor's reason for doing it? Outcome (choose one) What would be the resulting effect be? Mat would the information asset's security requirements be breached? Likelihood (choose one) High: Severity How severe are the consequences to the organization or sure in consequences to the organization on swell cause not detecting objects and possible, possibly other sensors can cover, yielden spots mage recorded by the cameras. Blind in cause not detecting objects and possible, possibly other sensors can cover, yielden spots mage recorded to the input is optimized. ing the sensor available without any ons will cause the system to not see ide, possibly other sensors can cover, yield amage the camera's lens. Video and Image data Medium — Car can continue driving but can't recognize traffic lights An attacker uses their tools to send malicious optical shand blind cameras causing unwanted binding attacker uses their tools to send malicious optical shand blind cameras causing unwanted binding attacker uses their thoole and image data. An attacker with some previous experience and tools to cious optical inputs (laser etc.), tools to further destabilize send a short output and blind cameras causing unwanted and confusion for longer period on the cameras and possibility and blind cameras causing unwanted and confusion for longer period on the cameras and possibility and blind cameras causing unwanted send image the camera sensors Wants disrupt the AV program to keep drivers' jobs. Wants disrupt the AV program to keep drivers' jobs. Wants disrupt the AV program to keep drivers' jobs. Wants disrupt the AV program to keep drivers' jobs. Wants disrupt the AV program to keep drivers' jobs. Wants disrupt the AV program to keep drivers' jobs. Wants disrupt the AV program to keep drivers' jobs. Wants disrupt the AV program to	

Risk Mitigation	R7 – Confusin	g controls wit	h attack on ca	mer	as				
Choose action to take.	Accept:								
For the risk, what actions and controls will be used:									
Layer where applied	ayer where applied Description of control or action Estimated cost								
Perception	Overlapping image output with multiple cameras Low								
Perception	Filter to remove ha	Filter to remove harmful light High							

Allegi	ro – Worksheet 10				k on LiD	AR				
	Business Asset	Surro	ound	ling environ	ment data					
	Business Asset's Value	High	1 – W	Vithout Surr	ounding env	rironment da	ita, car canno	t continue		
	Area of Concern	the in	nfori confu	mation got b usion, errors	y the LIDA	R to carry or	wave and man ut the relay at f surrounding	tack caus-		
	Actor Who would exploit the area of concern or threat?	with	spec	eific (905nn	n) waveleng	ths, oscilloso				
sat	Means How would the actor do it? What would they do?	confu unwa	using antec	g and manip d errors	ulating the d	lata received	carry out a relation by the LIDA	elay attack R causing		
Threat	Motive What is the actor's reason for doing it?	Wan	Wants disrupt the AV program to keep drivers' jobs.							
	Outcome (choose one) What would be the resulting		Disclosure:			Destr	ruction:			
	effect be?			Modification: x			Interruption:			
	Security Requirements How would the information asset's security requirements be breached?	LIDA	AR's	are not rela	y attack res	istant.				
	Likelihood (choose one)	Hig	h:		Medium:		Low:	X		
What a	equences re the consequences to the organ a result of the risk?	niza-	Hov owr	ier by impa	ct area?		e organizatio 1d 1 for lowes			
	attack will manipulate with the d by the LiDAR. This causes error			oact area		Priority*	Impact	Score		
the syst	em and possible accidents in the	traf-	Cor	nfidentiality		1	Low	1		
	lled errors can cause shutdown of	the	Ava	ilability		3	High	6		
LiDAR Confide	entiality is unaffected.		Inte	grity		3	High	9		
	•	<u>I</u> _		Rela	ative risk	score:	ı	16		
						core (Rel x	likelihood):	16		

Risk Mitigation	R8 – Relay	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										
Perception	Multiple LiD	AR in	puts			High					
Perception	Random probing						Low				
Perception	Shorten pulse period Low						7				

Allegr	ro – Worksheet 10	R9	- Spoofin	g L	iDAR					
	Business Asset	surr	ounding env	ironr	nent data					
	Business Asset's Value	Hig	h – Without	Surre	ounding env	vironment da	ta, car cannot	continue		
	Area of Concern	DA		ironr	nent, that a	re not there	o create object and causing lo			
	Actor Who would exploit the area of concern or threat?		attacker with specific (90				and tools to scope.	end light		
ıt.	Means How would the actor do it? What would they do?		attacker uses R in the envi				o create objec	ts for LI-		
Threat	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]	Disclosure	:		Destr				
	effect be?	M	Iodificatio	n:		Interr	X			
	Security Requirements How would the information asset's security requirements be breached?	LID	LIDAR's are not spoofing resistant.							
	Likelihood (choose one)	Hig	gh:		Medium:		Low:	X		
What ar	re the consequences to the organ a result of the risk?	iza-	owner by in	прас	rt area?		e organization			
	g artificial objects seen by the LiD use unwanted errors in the syst		Impact area			Priority*	Impact	Score		
interrup	driving management and could lead to trafinterruptions and accidents.		Confidentia	ality		1	Low	1		
	on availability is there, but the at		Availabilit	y		2	Medium	4		
new arti	nt remove real objects and only a dificial ones. Entiality is not affected.	adds	Integrity			3	High	9		
Connac	mining is not directed.		l	Re	lative ris	k score:		14		
				_			x likelihood):	14		
				10	TATION L	JOI O (Mel)	·			

Risk Mitigation	R9 – Spoo	R9 – Spoofing LiDAR									
Choose action to take.							Transfer:				
For the risk, what actions and controls will be used:											
Layer where applied	Description of control or action										
Perception	Multiple LiD	AR inp	outs			High					
Perception	Random probing						Low				
Perception	Shorten pulse period					Low					

Allegi	ro – Worksheet 10	R10) – (Code m	odi	ification				
	Business Asset	syste	em s	oftware						
	Business Asset's Value	High	1 – s	oftware is	s res	sponsible fo	r controlling	g 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?							vith car diagno e system code		
± .	Means How would the actor do it? What would they do?						e and tools and poten	to modify co	ode in the	
Threat	Motive What is the actor's reason for doing it?	Wan	Wants disrupt the AV program to keep drivers' jobs.							
	Outcome (choose one) What would be the resulting	Ι	Disc	losure:			Destruction:			
	effect be?	M	odi	odification: x Interruption:						
	Security Requirements How would the information asset's security requirements be breached?	Syste	em s	software c	can l	be modified	l, no validat	ion.		
	Likelihood (choose one)	Hig	h:			Medium:		Low:	X	
What a	equences re the consequences to the organ a result of the risk?	niza-	Ho	ner by im	раст	t area?		e organization		
	ing the code will cause unwanted can possibly be used to harm the			pact area	_		Priority*	Impact	Score	
or other Depend	r road users. ling on the modified code, it can be		Cor	nfidential	ity		1	Medium	2	
	the system making it unavailable to use.			ailability			3	High	9	
	he tools will allow the attacker to e used in the system.	see		egrity			2	High	6	
	•	Relative risk score:					17			
				1	To	Total Risk Score (Rel x likelihood): 17				

Risk Mitigation	R10 – Cod	R10 – Code modification									
Choose action to take.	Accept:	Accept: Defer: Mitigate: x Transfer:									
For the risk, what actions and controls will be used:											
Layer where applied	Description of control or action										
Application	Device authe	nticati	on			Med	ium				
Application	Anti-malwar	Anti-malware Low									
Application	Isolation Medium										

Allegr	o – Worksheet 10	R1	1 – Code	inje	ction					
	Business Asset	syst	em softwa	re						
	Business Asset's Value	Hig	h – softwar	e is re	sponsible fo	or controlling	g 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?		ing can use				vith car diagno mful code into			
t	Means How would the actor do it? What would they do?					e and tools to nd potential	inject code i harm.	n the sys-		
Threat	Motive What is the actor's reason for doing it?	Waı	Wants disrupt the AV program to keep drivers' jobs.							
	Outcome (choose one) What would be the resulting]	Disclosur	e:		Destr				
	effect be?	Modification: x			Interr	Interruption:				
	Security Requirements How would the information asset's security requirements be breached?	Har	Modification: x Interruption: Harmful code can be injected into system software, no valid							
	Likelihood (choose one)	Hig	gh:		Medium:		Low:	X		
What ar	quences re the consequences to the organ result of the risk?	iza-	owner by	ere are impac	t area?		e organization			
	g any kind of harmful code into will cause impacts to confidentia		Impact ar			Priority*	Impact	Score		
lect con	and availability. The code could fidential data, shut down parts of	the	Confiden	tiality		1	High	3		
	cause wrong decisions in the cont		Availabil	ity		2	High	6		
but can	ing of the cars. All this impacts the business out can also harm other road users when the ear is on the move.					3	High	9		
15 31				Rela	tive risk	score:		18		
			Total Risk Score (Rel x likelihood):							

Risk Mitigation	R11 – Cod	R11 – Code injection									
Choose action to take.	Accept:	De	fer:	Mitigate	e: x	Transfer:					
For the risk, what actions and controls will be used:											
Layer where applied	Description of control or action										
Application	Device auther	ntication			Med	Medium					
Application	Anti-malware	Anti-malware Low									
Application	Isolation	Isolation Medium					·				

Allegr	o – Worksheet 10	R 1	2 – Packet	sn	iffing					
	Business Asset	Con	nmunication	data	ì					
	Business Asset's Value	Hig	h - without c	omr	nunication th	ne componer	nts 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	ар	acket sniffer	and some pr	revious exper	ience.		
ıt	Means How would the actor do it? What would they do?		attacker uses nmunications			to intercept	and collect of	lata from		
Threat	Motive What is the actor's reason for doing it?	Wai	Wants to gather classified data to sell to competitors.							
	Outcome (choose one) What would be the resulting]	Disclosure	:	X	Destr	uction:			
	effect be?	M	Iodification	uption:						
	Security Requirements How would the information asset's security requirements be breached?	Con	Communication can be intercepted.							
	Likelihood (choose one)	Hig	gh:		Medium:	X	Low:			
What a	quences re the consequences to the organ a result of the risk?	iza-	owner by in	пра	ct area?		e organization			
	cket sniffer can gather data with		Impact area		1	Priority*	Impact	Score		
tion or 1	erruptions in a system with no de mitigation. The data communicate em can be confidential and harmfo	d in	Confidentia	ality		3	High	9		
wrong l	nands.		Availability	y		1	Low	1		
terruption	ly installed sniffer won't cause any ons in the communications and average s not affected.	y in- vail-				2	Low	2		
	sniffing does not affect the integrit munication (data will still be the s riginal).									
				R	elative risl	score:		12		
				Total Risk Score (Rel x likelihood):						

Risk Mitigation	R12 – Pac	ket sr	niffing						
Choose action to take.	Accept:		Defer:		Mitigate:	X	Transfer:		
For the risk, what actions and controls will be used:									
Layer where applied	Description	Description of control or action							
Network	Encryption					Medium			
Network	Device authentication					Medium			
Network	User authentication					Medium			

Allegi	ro – Worksheet 10	R 1	3 –]	Pack	et fuz	zing			
	Business Asset	Con	nmuı	nicatio	n data				
	Business Asset's Value	Hig	h - w	ithout	comm	nunication tl	ne compone	nts can't work	together
	Area of Concern	and	pote	ntially	expo		les in the so	ausing unwan ecurity causin	
	Actor Who would exploit the area of concern or threat?	An	attac	ker wi	th som	ne experienc	e working v	vith data pack	ages.
±	Means How would the actor do it? What would they do?							valid data to the sing security l	
Threat	Motive What is the actor's reason for doing it?	Wai	its to	find l	loopho	les and caus	se errors in t	he vehicle.	
	Outcome (choose one) What would be the resulting		Disclosure:				Destruction:		
	effect be?	M	Modification: x Interruption:						
	Security Requirements How would the information asset's security requirements be breached?	System can't handle invalid d			invalid data	inputs.	·		
	Likelihood (choose one)	Hig	gh:			Medium:		Low:	X
What a	equences re the consequences to the organ a result of the risk?	iza-	Ho	ner by	ere are impac	t area?		e organization	
	t any input validation, tempering nication data will cause errors in		Imp	oact ar	ea		Priority*	Impact	Score
loophol	The outcomes could be used to les in the security for other attack	s or	Coi	nfiden	tiality		3	High	9
	anipulating the vehicle to attac	kers	Av	ailabil	ity		1 Medium		2
control	·		Integrity				2	4	
		Relative risk score:				15			
		Total Risk Score (Rel x likelihood):					15		

Risk Mitigation	R13 – Packet fuzzing										
Choose action to take.	Accept:	Accept: Defer: Mitigate: x Transfer:									
For the risk, what actions and controls will be used:											
Layer where applied	Description of control or action										
Network	Encryption			Higl	h						
Network	Device authentication Medium										
Network	User authenti	User authentication Medium									

Business Asset Business Asset's Value Area of Concern An attacker uses their tools and motivation to listen gaining access to communication data Actor Who would exploit the area of concern or threat? Means How would the actor do it? What would they do? Motive What is the actor's reason for doing it? Communication data High - without communication the components can't want tools and motivation to listen gaining access to communication data An attacker uses their tools and motivation to listen gaining access to communication data Wants to gather classified data to sell to competitors.	o CAN bus, oss of confi- bus messages
Area of Concern An attacker uses their tools and motivation to listen gaining access to communication data and causing the dentiality of communication data Actor Who would exploit the area of concern or threat? Means How would the actor do it? What would they do? Motive What is the actor's reason for doing it? An attacker uses their tools and motivation to listen gaining access to communication data Wants to gather classified data to sell to competitors.	o CAN bus, oss of confi- bus messages
gaining access to communication data and causing the dentiality of communication data Actor Who would exploit the area of concern or threat? Means How would the actor do it? What would they do? Motive What is the actor's reason for doing it? gaining access to communication data and causing the dentiality of communication data An attacker with tools and motivation to listen gaining access to communication data Wants to gather classified data to sell to competitors.	oss of confi- ous messages
Actor Who would exploit the area of concern or threat? Means How would the actor do it? What would they do? Motive What is the actor's reason for doing it? An attacker with tools and motivation to listen to CAN in the concern or threat? An attacker uses their tools and motivation to listen gaining access to communication data Wants to gather classified data to sell to competitors.	
How would the actor do it? What would they do? Motive What is the actor's reason for doing it? What is the actor's reason for doing it? Was to gather classified data to sell to competitors.	to CAN bus
doing it?	
Outcome (choose one) What would be the resulting Disclosure: x Destruction:	
effect be? 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 as a result of the risk? with the consequences to the organization as a result of the risk? sometimes to the organization as a result of the risk? sometimes to the organization as a result of the risk? sometimes to the organization as a result of the risk?	
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 Confidentiality 3 High	9
channel of many different ones. Availability 1 Low	1
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.	2
Relative risk score:	12
Total Risk Score (Rel x likelihood	

Risk Mitigation	R14 -Eave	R14 –Eavesdropping CAN										
Choose action to take.	Accept:	Accept: Defer: Mitigate: x Transfer:										
For the risk, what actions and controls will be used:												
Layer where applied	Description of control or action											
Network	Encryption					High	1					
Network	Device authentication Medium											
Network	User authent	User authentication Medium										

Allegr	o – Worksheet 10	R15	5– I	nject (CAN	N message	es			
	Business Asset	Com	nmur	nication	data					
	Business Asset's Value	High	1 - W	ithout c	omn	unication th	ne componer	nts can't worl	together	
	Area of Concern	ance	s in	the syst	em a		accidents a	ssages causin and causing tl		
	Actor Who would exploit the area of concern or threat?	An a	ittac]	ker with	tool	s to inject C	CAN messag	es.		
+	Means How would the actor do it? What would they do?		An attacker uses their tools to inject CAN messages causing ances in the system and possible accidents.							
Threat	Motive What is the actor's reason for doing it?	Wan	ıts di	srupt the	e AV	⁷ program to	keep drive	rs' jobs.		
	Outcome (choose one) What would be the resulting		Disclosure:			X	Destruction:			
	effect be?	M	Modification: Interruption:							
	Security Requirements How would the information asset's security requirements be breached?	No authentication			n for	· CAN mess	ages.			
	Likelihood (choose one)	Hig	gh:			Medium:	m: Low: x			
What a	quences re the consequences to the organ a result of the risk?	niza-	Ho	ner by in	прас	t area?		e organization		
	g CAN messages will cause error tem and possible accidents. Inv			act area			Priority*	Impact	Score	
message planner	es cause wrong decisions by drivand harm to the vehicle or passen	ving	Cor	nfidentia	lity		2	Medium	4	
is possil		. [ailability	1		1	Medium	2	
	ssages can be used to shut down components.	1m-	Inte	egrity			3	High	9	
			Relative risk score:					15		
					To	tal Risk S	Score (Rel :	x likelihood):	15	

Risk Mitigation	R15– Inje	R15– Inject CAN messages									
Choose action to take.	Accept:	Accept: Defer: Mitigate: x Transfer:									
For the risk, what actions	actions and controls will be used:										
Layer where applied	Description of control or action										
Network	Encryption					High	า				
Network	Device authentication Medium										
Network	User authentication Medium										

Allegi	ro – Worksheet 10	R1	6 – GPS	jamr	ning and	spoofing					
	Business Asset	Loc	ation data								
	Business Asset's Value					essential for					
	Area of Concern	GPS	S, making t	the ve			ified signals to essible and ca				
	Actor Who would exploit the area of concern or threat?				ls to send G	PS signals.					
;	Means How would the actor do it? What would they do?		An attacker can use their tools to send modified signals to GPS, making the vehicle localization not possible.								
Threat	Motive What is the actor's reason for doing it?	Waı	nts disrupt	the A	V program to	o keep drive	rs' jobs.				
	Outcome (choose one) What would be the resulting]	Disclosur	e:		Destr					
	effect be?	M	Modification: Interruption:								
	Security Requirements How would the information asset's security requirements be breached?	GPS	S in not jan	nming	resistant.		<u>'</u>				
	Likelihood (choose one)	Hig	gh:		Medium:	X					
What a	equences re the consequences to the organ a result of the risk?	iza-	owner by	re are impac	ct area?		e organization				
	the integrity of data will cause the make wrong decisions and poter		Impact ar	ea		Priority*	Impact	Score			
Not hav	oother road users. ving the sensor available without		Confiden	tiality		1	Low	1			
	ions will cause the system to not		Availabil	ity		3	High	9			
	side, possibly other sensors can co		Integrity			2	High	6			
			ı	Rela	ative risk	score:	l	16			
						core (Rel x	likelihood):	32			

Risk Mitigation	R16 – GPS jai	R16 – GPS jamming									
Choose action to take.	Accept:	Accept: Defer: Mitigate: x Transfer:									
For the risk, what actions and controls will be used:											
Layer where applied	Layer where applied Description of control or action Estimated cost										
Perception	Nullification High										
Perception	Monitoring signal	s and identifica	tion nodes	Med	lium						

Allegi	ro – Worksheet 10	R1	7 – EMP a	ittac	eks			
	Business Asset	Aut	onomous dri	ving				
	Business Asset's Value	Hig	h – Without	autor	nomous driv	ing, it is a n	ormal car	
	Area of Concern	AV		onom	ous driving	impossible	wn componer and causing the	
	Actor Who would exploit the area of concern or threat?	An	attacker with	EM	P generator			
ıt	Means How would the actor do it? What would they do?		attacker uses , making auto				wn componer	nts in the
Threat	Motive What is the actor's reason for doing it?	Waı	nts disrupt th	e AV	program to	keep drive	rs' jobs.	
	Outcome (choose one) What would be the resulting]	Disclosure	•		Destr	ruction:	
	effect be?	M	Modification: Interruption:					
	Security Requirements How would the information asset's security requirements be breached?	Elec	ctronic comp	onen	ts in AV ca	n be affected	d with EMP.	
	Likelihood (choose one)	Hig	gh:		Medium:		Low:	X
What a	equences re the consequences to the organ a result of the risk?	iza-	owner by in	прас	t area?		e organizatior	
	ttacks can shut down component. Depending on the pulse genera		Impact area			Priority*	Impact	Score
affect v	act is different. Small pulse may cery small components but bigger of	ones	Confidentia	ality		1	Low	1
	ect larger components and even ca					3	High	9
	ent damage. Generating high implies hard and the tools used are exp		Integrity			2	Low	2
				Re	lative ris	k score:	1	12
				To	tal Risk S	Score (Rel :	x likelihood):	12

Risk Mitigation	R17 – EMP att	R17 – EMP attacks										
Choose action to take.	Accept:	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	Isolation Medium										

Allegr	ro – Worksheet 10	R1 3	8 – Injec	t ma	lware					
	Business Asset	Aut	onomous d	lriving						
	Business Asset's Value	Hig	h – Withou	ıt auto	nomous driv	ing, it is a n	ormal car			
	Area of Concern	syst of a	em, causin utonomous	g erro drivi	rs, loss of d	ata, acciden	inject malwarts and loss of	integrity		
	Actor Who would exploit the area of concern or threat?	An	attacker wi	th acc	ess to ports	or network t	o inject malw	are.		
ıt	Means How would the actor do it? What would they do?	An a		es phy	sical ports o	r network to	inject malwa	re into the		
Threat	Motive What is the actor's reason for doing it?				alware, the and so on.	attacker can	gather classi	fied data,		
	Outcome (choose one) What would be the resulting	Disclosure:			Destr	X				
	effect be?	M	Modification: Interruption:							
	Security Requirements How would the information asset's security requirements be breached?	Phy	sical port o	or netv	vork can be	used to injec	et malware.			
	Likelihood (choose one)	Hig	gh:		Medium:	X				
What a	equences re the consequences to the organ a result of the risk?	iza-	owner by	ere are impa	ct area?		e organization			
of troub	malware in the system can cause able. Having affected the system, it	will	Impact ar	rea		Priority*	Impact	Score		
have the	er to add more malware. All of this e attacker gather data, disturb the d	riv-	Confiden	tiality		3	High	9		
	cess, causing harm to the component	ents	ents Availability			2	High	6		
	on. outcome is the destruction of the us driving process.	au-	Integrity	-		1	High	3		
	<u> </u>	Relative risk score:						18		
		Total Risk Score (Rel x likelihood):						36		

Risk Mitigation	R18 – Inje	R18 – Inject malware										
Choose action to take.	Accept:	Accept: Defer: Mitigate: x Transfer:										
For the risk, what actions and controls will be used:												
Layer where applied	Description of control or action											
Application, Network	Install firewa	.11				Low	1					
Application	Anti-malware Low											
Application	Isolation	Isolation Medium										

Allegi	ro – Worksheet 10	R19) _]	Manipula	te map da	ıta				
	Business Asset	Map	data	a						
	Business Asset's Value	High	1 – N	Aap is requi	ed to know	where roads	are			
	Area of Concern		n tra				nanipulate the loss of integri			
	Actor Who would exploit the area of concern or threat?	An a	ittac	ker with acc	ess to the sto	orage and m	aps.			
1	Means How would the actor do it? What would they do?			ker uses thei affic disturba			nanipulate the	m, result-		
Threat	Motive What is the actor's reason for doing it?	Wan	Wants disrupt the AV program to keep drivers' jobs.							
	Outcome (choose one) What would be the resulting	Γ	Disc	losure:		Destruction:				
	effect be?	M	odi	fication:	Х	Interruption:				
	Security Requirements How would the information asset's security requirements be breached?	Stora	age a	and map dat	a are not aut	henticated.	,			
	Likelihood (choose one)	Hig	h:		Medium:		Low:	X		
What a	equences re the consequences to the organ a result of the risk?	niza-	Ho	ner by impa	ct area?		e organizatio			
	ata is crucial for the vehicle to kn and how it should drive. Manipula		_	pact area		Priority*	Impact	Score		
the line	es used to locate the car on the st nake the car drive on sideways or e	treet	Coı	nfidentiality		2	Low	2		
hit obje		ŀ	Ava	ailability		1	Low	1		
		Integrity				3	High	9		
				Rela	ative risk	score:		12		
				Tot	al Risk So	core (Rel x	likelihood):	12		

Risk Mitigation	R19 – Mai	nipul	ate map da	ata					
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					Med	ium		
Application	Device authe	Device authentication Medium							
Application	User authent	User authentication Medium							

Allegi	ro – Worksheet 10	R20	0 – 1	Extract m	ap data			
	Business Asset	Map	data	ı				
	Business Asset's Value	High	h – N	Iap is requi	red to know	where roads	are	
	Area of Concern						nanipulate the	
		ing i	in in	formation le	ak and loss	of confident	iality of map	data.
	Actor Who would exploit the area of concern or threat?	An a	attac]	ker with acc	ess to the st	orage and m	aps.	
	Means How would the actor do it? What would they do?		An attacker uses their access to the maps to extract them, information leak.					
Threat	Motive What is the actor's reason for doing it?	War	nts di	srupt the A	V program t	o keep drive	rs' jobs.	
	Outcome (choose one) What would be the resulting		Disc	losure:	X	Destr	ruction:	
	effect be?	M	Modification: Interruption:					
	Security Requirements How would the information asset's security requirements be breached?	Stor	age a	and map dat	a are not au	thenticated.	,	
	Likelihood (choose one)	Hig	gh:		Medium		Low:	X
What a	re the consequences to the organ a result of the risk?	niza-	Ho	ner by impa	ct area?		e organizatio	
	g access to the map data will cause risks in other aspects. Knowing v		Imp	oact area		Priority*	Impact	Score
	d what streets will most likely be used by the attacker to prepare o		Coı	nfidentiality		3	High	9
attacks.		-	Ava	ailability		1	Low	1
Selling	of the data is possible.	•	Integrity			2 Low		2
		Relative risk score:					12	
				Tot	al Risk S	core (Rel x	likelihood):	12

Risk Mitigation	R20 – Ext	ract r	nap 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								
Application	Isolation					Med	ium		
Application	Device authe	Device authentication Medium							
Application	User authent	ication		·	•	Med	ium		

Allegi	ro – Worksheet 10	R2	1 –]	Delete ma	p data				
	Business Asset	Map	data	a					
	Business Asset's Value	Higl	h – N	Aap is requir	ed to know	where roads	are		
	Area of Concern		ic di				lelete them, ro of availabili		
	Actor Who would exploit the area of concern or threat?	An a	attac	ker with acc	ess to the st	orage and m	aps.		
1 2	Means How would the actor do it? What would they do?		An attacker uses their access to the maps to delete them, resulting traffic disturbances and accidents.						
Threat	Motive What is the actor's reason for doing it?	War	Wants disrupt the AV program to keep drivers' jobs.						
	Outcome (choose one) What would be the resulting	I	Disclosure:			Destr	Destruction:		
	effect be?	Modification:			Interruption:				
	Security Requirements How would the information asset's security requirements be breached?	Storage and map data are not authenticated.							
	Likelihood (choose one)	Hig	gh:		Medium:		Low:	X	
What a	equences re the consequences to the organ a result of the risk?	niza-	Ho	ner by impac	ct area?		e organizatio		
	tta is crucial for autonomous driv		Imp	pact area		Priority*	Impact	Score	
and cor	ntinuing the work is impossible uta is provided.		Coı	nfidentiality		2	Low	2	
				ailability		3	High	9	
		Integrity			1 Low		1		
				Rela	ative risk	score:		12	
				Tota	al Risk So	core (Rel x	likelihood):	12	

Risk Mitigation	R21 – Dele	te map data							
Choose action to take.	Accept:	Defer:	X	Transfer:					
For the risk, what actions and controls will be used:									
Layer where applied	Description	Description of control or action							
Application	Isolation			Medium					
Application	Device auther	Device authentication Medium							
Application	User authentic	cation		Med	lium				

Allegr	ro – Worksheet 10	R22	2 –]	Disabl	e ac	tuation n	odule		
	Business Asset	Auto	onon	nous dri	ving				
	Business Asset's Value	High	h - V	Vithout	autor	nomous driv	ing, it is a n	ormal car	
	Area of Concern		ble tl					on module, w ilability of aut	
	Actor Who would exploit the area of concern or threat?	An a	attac	ker who	can	install malv	vare on the a	actuation mod	ule.
it.	Means How would the actor do it? What would they do?		An attacker installs malware on the actuation module, which c disable the functions of it.						hich can
Threat	Motive What is the actor's reason for doing it?	War	ants disrupt the AV program to keep drivers' jobs.						
	Outcome (choose one) What would be the resulting		Disclosure:			Destruction:			
	effect be?		Modification:				Interr	ruption:	X
	Security Requirements How would the information asset's security requirements be breached?	Actuation modu			le is 1	not theft pro	oof.		
	Likelihood (choose one)	Hig	gh:			Medium:		Low:	X
What a	equences re the consequences to the organ a result of the risk?	niza-	Ho	ner by in	прас	t area?		e organization	
	on module is responsible to carry trols given by computing unit. W			pact area			Priority*	Impact	Score
out it, a Disablii	utonomous driving is impossible. ng the actuation module can be u	ısed	Coı	nfidentia	ality		1	Low	1
to dema	and money for the malware remov	al.		ailabilit	у		3	High	9
			Integrity			2 Medium		4	
				Relative risk so			sk score:		14
		Total Risk Score (Rel x likelihood				x likelihood):	14		

Risk Mitigation	R22 – Disable	actuation mod	ule						
Choose action to take.	noose 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 acti	ion	Est	imated cost				
Application	Isolation			Med	lium				
Application	Access Control			Low	,				

Allegi	ro – Worksheet 10	R2.	3 – Ind	uce ba	d analysis	S		
	Business Asset	Aut	onomous	driving				
	Business Asset's Value	Hig	h – Witho	out auto	nomous driv	ing, it is a n	ormal car	
	Area of Concern	war	e causing	the car	to follow a		Take output of ers and causing ter	
	Actor Who would exploit the area of concern or threat?					he used soft		
;	Means How would the actor do it? What would they do?					e to create f tackers orde	fake output of ers.	the soft-
Threat	Motive What is the actor's reason for doing it?	program to	o keep drive					
	Outcome (choose one) What would be the resulting	Disclosure:				Destr		
	effect be?		Iodifica	tion:	X	Interruption:		
	Security Requirements How would the information asset's security requirements be breached?	Soft	tware in c	omputii	ng unit is no	t protected.		
	Likelihood (choose one)	Hig	gh:		Medium:		Low:	X
What a	equences re the consequences to the organ a result of the risk?	iza-	owner b	vere are vy impac	rt area?		e organization	
	ng bad analysis makes the vehicle to led by the attacker. The attacker		Impact			Priority*	Impact	Score
ation m	what inputs will be given to the a nodule, as they know what the in		Confide	entiality		1	Low	1
	how they would be used.		Availab			2	Medium	4
harm to	an attacker control the car can can the car itself, passengers or other and their property.		Integrity	у		3	High	9
asors ar	and property.	Relative risk score:						14
			ŀ				kelihood):	14
		Total Risk Score (Rel x likelihood):						

Risk Mitigation	R23 – Indu	ce bad analys	sis							
Choose action to take.	Accept:	Defer:		Mitigate:	X	Transfer:				
For the risk, what actions and controls will be used:										
Layer where applied	Description	Description of control or action								
Application	Isolation				Med	lium				
Application	Access Contro	Access Control Low								
Application	Input validation	on			Low	,	·			

II. Validated OCTAVE Worksheets

Allegi	ro – Worksheet 10	R4	– Ja	mming	g ra	adar			
	Business Asset	Surr	oundi	ng envii	roni	nent data			
	Business Asset's Value	Low	-Lo	sing rad	lar d	data does n	ot impact B	OLT AV	
	Area of Concern	rada	r caus		e bla	ackout on th		ne data receive loss of integri	
	Actor Who would exploit the area of concern or threat?					e previous of plier etc.).	experience v	vith radars and	l has sig-
at	Means How would the actor do it? What would they do?	attacing to 77G	An attacker uses their knowledge and tools to carry out a jamm attack on radar by emitting frequencies used by the sensors and caing false information (distance constantly changing) received (77GHz in the experiment).						
Threat	Motive What is the actor's reason for doing it?				AV	program to	keep drive		
	Outcome (choose one) What would be the resulting	Disclosure:				Destru		uction:	
	effect be?		Modification:				Interr	uption:	X
	Security Requirements How would the information asset's security requirements be breached?	Radars are not ja			nmi	ng resistant			
	Likelihood (choose one)	Hig	gh:			Medium:	X	Low:	
What a tion as	equences re the consequences to the organ a result of the risk?		How owne *3 fc	er by im or highes	рас	t area?	r medium an	e organization	
	the integrity of data will cause the make wrong decisions and poten		Impa	act area			Priority*	Impact	Score
harm to Not hav	o other road users. ving the sensor available without	any	Conf	fidential	ity		1	Low	1
	ions will cause the system to not				3	High	9		
	side, possibly other sensors can co ng attack on radar will not cause aks.		Integ	grity			2	High	6
					Relative risk score:				16
					To	tal Risk S	Score (Rel	x likelihood):	32

Risk Mitigation	R4 – Jami	ning	radar						
Choose action to take.	Accept:		X	Transfer:					
For the risk, what actions and controls will be used:									
Layer where applied	Descriptio	n of c	control or	actio	n	Est	imated cost	ţ	
Perception	Noise detecti	on and	rejection			Low	7		
Perception	Multiple sens	sors for	r redundancy	check		Low	7		

Allegr	o – Worksheet 10	R5	$-S_1$	poofin	g ra	adar				
	Business Asset Business Asset Surrounding environment data 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? Means How would the actor do it? What would they do? Motive What is the actor's reason for doing it? Outcome (choose one) What would be the resulting effect be? Modification: Radars are not spoofing resistant. Medium: x Low:									
	Business Asset's Value									
	Area of Concern	rada	ır cau	ising co	nsta	nt changes in	n distance/ve	elocity on the		
	Who would exploit the area of						experience v	vith radars and	d has sig-	
at	How would the actor do it?	atta	ck on false	radar b inform	y en	nitting freque	encies used b	y the sensors	and caus-	
Thre	What is the actor's reason for	Wai	nts di	srupt th		V program t	o keep drive	rs' jobs.		
	What would be the resulting	Disclosure:			•		Destruction:			
	effect be?	Modification		n:		Interr	uption:	X		
	How would the information asset's security requirements	Rad	ars a	re not sp	poof	ing resistant				
	Likelihood (choose one)	Hig	gh:			Medium:	X	Low:		
What ar	quences re the consequences to the organ result of the risk?		Hov owr *3 j	ıer by ir for high	npac est p	ct area?	r medium an	e organization nd 1 for lowes		
tem to	he integrity of data will cause the make wrong decisions and poten		Imp	act area	ı		Priority*	Impact	Score	
Not hav	other road users. ring the radar available without		Cor	nfidentia	ality		1	Low	1	
	ons will cause the system to not			ailability	y		2	High	6	
	ide, possibly other sensors can cog attack on radar will not cause ks.		Inte	egrity			3	High	9	
					Re	elative ris	k score:		16	
					: likelihood):	32				

Risk Mitigation	R5 – Spoofing radar								
Choose action to take.	Accept:	Accept: Defer: Mitigate: x Transfe							
For the risk, what actions and controls will be used:									
Layer where applied	Layer where applied Description of control or action Estimated cost								
Perception	Preption Noise detection and rejection Low								
Perception	Multiple sensor	s for redundancy	check		Low	7			

Allegi	ro – Worksheet 10	R7	– Confu	sing o	controls v	vith attac	k on came	as	
	Business Asset	Vide	eo and Ima	ge data	a				
	Business Asset's Value	Hig	h – Image	recogi	nition is ess	ential for sa	ıfe driving		
	Area of Concern	and long	blind cam	eras ca possib	ausing unwa ole hardwar	anted blindr	us optical shoness and confind loss of in	usion for	
	Actor Who would exploit the area of concern or threat?						and tools to s er destabilize		
eat	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. Mess with image recognition to cause accidents.							
Threat	Motive What is the actor's reason for								
	doing it? Outcome (choose one) What would be the resulting	I	Disclosur	e:		Destruction:			
	effect be?	M	Modification			Interruption:		X	
	Security Requirements How would the information asset's security requirements be breached?	Can	neras are vi	ulnerable to blinding attacks.					
	Likelihood (choose one)	Hig	gh: x		Medium:		Low:		
What a tion as	equences re the consequences to the organ a result of the risk?		owner by *3 for hig	re are impac hest p	t area?	r medium ar	e organization	t	
	asers to carry out the attack can ly damage the camera's lens.	per-	Impact ar	ea		Priority*	Impact	Score	
Messin sure w	g with camera inputs and auto exill make it harder to detect tra	affic	Confiden	iality		1	Low	1	
	signs and pedestrians. More likel	ely to Availability			3	High	9		
cause a	ccidents.		Integrity			2 High		6	
		Relative risk			k score:	16			
				To	tal Risk S	core (Rel x	: likelihood):	48	

Risk Mitigation										
Choose action to take.	Accept:	Accept: Defer: Mitigate: x Transfer:								
For the risk, what actions and controls will be used:										
Layer where applied	Layer where applied Description of control or action Estimated cost									
Perception	ion Overlapping image output with multiple cameras Low									
Perception	Turn off auto exposure Low									

Alleg	ro – Worksheet 10	R8	- Relay	attac	k on LiD	AR				
	Business Asset	Suri	rounding e	nviron	ment data					
	Business Asset's Value	Hig	h – Withou	ıt Surr	ounding env	ironment da	ta, car canno	t continue		
	Area of Concern	the ing	information confusion,	n got b errors <i>nipula</i>	y the LIDA and loss o ating with th	R to carry ou f integrity of	wave and man at the relay att f surrounding aputs could po	tack caus-		
	Actor Who would exploit the area of concern or threat?	with	n specific (905nm	n) waveleng	ths, oscilloso	cope.	tools to send light		
Threat	Means How would the actor do it? What would they do?	An attacker uses their knowledge and tools to carry out a relay atta confusing and manipulating the data received by the LIDAR causi unwanted errors.								
Th	Motive What is the actor's reason for doing it?	Wai	nts disrupt	rs' jobs.						
	Outcome (choose one) What would be the resulting		Disclosure:			Destr				
	effect be?	N.	Modification:		Х	Interr	uption:			
	Security Requirements How would the information asset's security requirements be breached?									
	Likelihood (choose one)	Hig	gh:		Medium:		Low:	X		
What a	equences are the consequences to the organ a result of the risk?	iiza-	owner by	ere are impac	ct area?		e organizatio			
	ying LiDAR inputs in certain way d to control the car by an attacker.	can	Impact as	rea		Priority*	Impact	Score		
	•		Confidentiality			1	Low	1		
		Availability			3	High	6			
			Integrity			3	9			
				-	ative risk			16		
		Total Risk Sco				core (Rel x	16			

Risk Mitigation	R8 – Rela	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 LiD	fultiple LiDAR inputs High								

Allegr	ro – Worksheet 10	R9	$-\mathbf{S}_{\mathbf{I}}$	poofin	g Li	DAR				
	Business Asset	surro	ound	ing env	ironn	nent data				
	Business Asset's Value	High	h-L	iDAR i	s prii	mary tool fo	or obstacle d	letection		
	Area of Concern	DAF	R in	the envi	ironn		e not there	o create object and causing l		
	Actor Who would exploit the area of concern or threat?	with	spec	cific (90)5nm		hs, oscilloso	and tools to scope.	send light	
1	Means How would the actor do it? What would they do?					r knowledge nent, that are		o create objec	ets for LI-	
Threat	Motive What is the actor's reason for doing it?	Wan	ıts di	srupt th	e AV	⁷ program to	keep drive	rs' jobs.		
	Outcome (choose one) What would be the resulting	Disclosi					Destruction:			
	effect be?	M	Modification:			Interr	ruption:	X		
	Security Requirements How would the information asset's security requirements be breached?	LIDAR's are not			spoo	ofing resista	nt.			
	Likelihood (choose one)	Hig	h:	x		Medium:		Low:		
What a	equences re the consequences to the organ a result of the risk?	niza-	Hov owr	ner by in	прас	t area?		e organizatio		
	g smoke clouds will cause the LiD of them as obstacles. Detecting s			act area			Priority*	Impact	Score	
smoke	with LiDAR can cause emerge and possible accidents because	ency	Cor	nfidentia	ality		1	Low	1	
that.	hat.			ailability	у		2	Medium	4	
				Integrity			3	9		
				Relative risk score:				14		
				Total Risk Sco				core (Rel x likelihood):		

Risk Mitigation	R9 – Spoofing	LiDAR			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 a	ction	Est	imated cost	t								
Perception Multiple LiDAR inputs High														
Perception	Better obstacle det	ection algorithr	ns	Low	,									

Allegi	ro – Worksheet 10	R 10	0 – 0	Code 1	nod	ification			
	Business Asset	Syst	tem s	software	;				
	Business Asset's Value	High	h – s	oftware	is res	sponsible fo	r controllin	g the car	
	Area of Concern	unw	ante	d chang	es an	d potential		he system code oss of integrit <i>ries</i> .	
	Actor Who would exploit the area of concern or threat?	codi	ing c	an use (OBD-			vith car diagno ne system code	
+	Means How would the actor do it? What would they do?	<i>it?</i> An attacker uses their knowledge and tools to mod system causing unwanted changes and potential harm							de in the
Threat	Motive What is the actor's reason for doing it?	War	nts di	isrupt th	ne AV program to keep drivers' jobs.				
	Outcome (choose one) What would be the resulting	Disclosure:		-		Destruction:			
	effect be?		Modification:			X	Interr	ruption:	
	Security Requirements How would the information asset's security requirements be breached?	System software ca				be modified	l, no validat	ion.	
	Likelihood (choose one)	Hig	gh:			Medium:		Low:	X
What a	equences re the consequences to the organ a result of the risk?	iza-	Ho	ner by in	прас	t area?		e organization	
	ng the code in the repository problems with all the cars using		Imp	pact area	a		Priority*	Impact	Score
same co			Coı	nfidentia	ality		1	Medium	2
harm to	arm to the next person in the car.			ailabilit	y		3	High	9
				egrity	,		2 High		6
			Relative ris			lative risl	k score:	17	
		Total Risk Score (Rel x likelihood):					17		

Risk Mitigation	R10 – Code modification									
Choose action to take.	Accept:	Defe	x Transfer:							
For the risk, what actions and controls will be used:										
Layer where applied	d Description of control or action Estimated cost									
Application	Unit tests				Low	7				
Application	Regular manual checks Low									
Application	Access contro	Access control Low								

Allegr	o – Worksheet 10	R1.	3 –]	Packet fu	zzing			
	Business Asset	Con	nmur	nication data	ı			
	Business Asset's Value	High geth		without con	nmunication	the comp	onents can't	work to-
	Area of Concern	and	pote		sing loopho	oles in the s	ausing unwan ecurity causir	
	Actor Who would exploit the area of concern or threat?	An a	attac	ker with son	ne experienc	e working v	vith data pack	ages.
at	Means How would the actor do it? What would they do?						valid data to the	
Threat	Motive What is the actor's reason for doing it?	War	nts to	find loopho	oles and caus	cause errors in the vehicle.		
	Outcome (choose one) What would be the resulting effect be?		Disclosure:			Destruction:		
			Modification: x			Interr	ruption:	
	Security Requirements How would the information asset's security requirements be breached?	System can't handle i			invalid data	inputs.		
	Likelihood (choose one)	Hig	gh:		Medium:		Low:	X
What a	quences re the consequences to the organ a result of the risk?	iza-	Ho	ner by impa	ct area?		e organization	
	t any input validation, tempering v nication data will cause errors in		Imp	pact area		Priority*	Impact	Score
system. loophol	The outcomes could be used to es in the security for other attack	find s or	Coı	nfidentiality		3	High	9
	inipulating the vehicle to attack	kers	Ava	ailability		1 2	Medium	2
control.	control.			Integrity			Medium	4
		Relative risk score:					15	
		Total Risk Score (Rel x likelihood): 15						

Risk Mitigation	R13 – Pac	ket fu	ızzing						
Choose action to take.	Accept: Defer: Mitigate:		x Transfer:						
For the risk, what actions and controls will be used:									
Layer where applied	re applied Description of control or action Estimated cost								
Network	Encryption					High			
Network	User authent	ication				Medium			
Network	Secure connection Medium								
Network	Split network	plit network (multiple smaller parts) Low							

Allegi	ro – Worksheet 10	R1	6 – 0	GPS jamı	ning						
	Business Asset	Location data									
	Business Asset's Value	Hig	h – K	Cnowing the	location is	essential for	AV				
	Area of Concern	GPS loss GPS	An attacker can use their tools to send modified signals to jam GPS, making the vehicle localization not possible and causing loss of integrity of location data. GPS also uses correction got in real-time which could be an atta opportunity.								
	Actor Who would exploit the area of concern or threat?	An attacker with tools to send GPS signals									
Threat	Means How would the actor do it? What would they do?	An attacker can use their tools to send modified signals to jam t 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?		Disc	losure:		Destr					
			Modification:			Interr	X				
	Security Requirements How would the information asset's security requirements be breached?	GPS in not jamming resistant.									
	Likelihood (choose one)	Hig	gh:		Medium:	X	Low:				
Consequences What are the consequences to the organtion as a result of the risk?		iza-	Severity How severe are the consequences to the organization owner by impact area? *3 for highest priority, 2 for medium and 1 for lowest								
	Losing the integrity of data will cause the tem to make wrong decisions and poten			pact area		Priority*	Impact	Score			
harm to other road users. The correction is used to get even less en			Cor	nfidentiality		1	Low	1			
	(from meters to few centimetres), mess			ailability		3	High	9			
with it	can cause accidents on the road.		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:	Accept: Defer: Mitigate: x Transfe								
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 fo	,								

Allegi	ro – Worksheet 10	R1	7 – EMP a	tta	cks					
	Business Asset	Aut	onomous dri	ving						
	Business Asset's Value	Hig	h – Without	auto	nomous driv	ving, it is a n	ormal car			
	Area of Concern	AV	An attacker uses EMP generator to shut down component AV, making autonomous driving impossible and causing the availability of autonomous driving.							
	Actor Who would exploit the area of concern or threat?	An	An attacker with EMP generator.							
;	Means How would the actor do it? What would they do?		An attacker uses EMP generator to shut down component AV, making autonomous driving impossible.							
Threat	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	•		Destr				
			Iodification	n:	Interruption:			X		
	Security Requirements How would the information asset's security requirements be breached?	Elec	ctronic comp	onen	its in AV ca	n be affected	d with EMP.			
	Likelihood (choose one)	Hig	gh:		Medium:		Low:	x		
What a	equences re the consequences to the organ a result of the risk?	iza-	owner by in	прас	rt area?		e organization			
	EMP attacks can shut down components the car. Depending on the pulse generate			a		Priority*	Impact	Score		
the imp	the impact is different. Small pulse may or affect very small components but bigger on		Confidentia	ality		1	Low	1		
can affect larger components and even cause			Tivaliaoliity			3	High	9		
permanent damage. Generating high impulses is hard and the tools used are exp sive.			Integrity			2 Low		2		
			1	Re	lative ris	k score:	<u> </u>	12		
				Total Risk Score (Rel x likelihood):				12		

Risk Mitigation	R17 – EMP attacks									
Choose action to take.	e action to take. Accept: x Defer: Mitigate: Transfer:									
For the risk, what actions and controls will be used:										
Layer where applied Description of control or action Estimated cost							t			

Allegi	ro – Worksheet 10	R19	9 –]	Mani	ipulat	te map da	ıta				
	Business Asset	Map	data	a							
	Business Asset's Value	High – Map is required to know where roads and signs/lights are									
	Area of Concern	sulti	An attacker uses their access to the maps to manipulate a sulting in traffic disturbances and accidents and loss of of map data								
	Actor Who would exploit the area of concern or threat?	An a	An attacker with access to the storage and maps. <i>Possibly inside</i>								
Threat	Means How would the actor do it? What would they do?		An attacker uses their access to the maps to manipulate them, reing in traffic disturbances and accidents.								
	Motive What is the actor's reason for doing it?	Wants disrupt the			the AV program to keep drivers' jobs.						
	Outcome (choose one) What would be the resulting effect be?		Disclosure:				Destr	Destruction:			
			Modification:			X	Interruption:				
	Security Requirements How would the information asset's security requirements be breached?	Storage and m			ap data	are not aut	henticated.	<u>'</u>			
	Likelihood (choose one)	Hig	ligh:			Medium:		Low:	x		
Consequences What are the consequences to the organ tion as a result of the risk?		niza-	Severity iza- How severe are the consequences to the organization or owner by impact area? *3 for highest priority, 2 for medium and 1 for lowest								
	nta is crucial for the vehicle to kn and how it should drive. Manipula			pact ar			Priority* Impact		Score		
the lines used to locate the car on the str could make the car drive on sideways or e			treet Confidentiality				2	Low	2		
hit obje	hit objects.			ailabil	ity		1 Low		1		
			Integrity				3 High		9		
			Relative risk score:					12			
		Total Risk Score (A					core ($\overline{Rel} x$	(Rel x likelihood):			

Risk Mitigation	R19 – Manipulate map data									
Choose action to take.	Accept:	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 sim	Low	7							