## I. Filled OCTAVE Worksheets

Allegi	ro – Worksheet 10	R1	– Jammir	ıg ul	trasonic	sensors		
	<b>Business Asset</b>	Ultr	asonic senso	rs dat	ta			
	<b>Business Asset's Value</b>	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?	An attacker uses their knowledge and tools to carry out a attack on ultrasonic ranging sensors by emitting frequencies the sensors and causing false information received by the s Wants disrupt the AV program to keep drivers' jobs.						
Threat	Motive What is the actor's reason for doing it?		•		program to	keep drive	rs' jobs.	
	Outcome (choose one) What would be the resulting	I	Disclosure	:		Destr	ruction:	
	effect be?	M	Modification:			Interr	ruption:	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			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		Availability	у		2	High	6
Jammir	side, possibly other sensors can co ng attack on ultrasonic sensor will ny data leaks.		Integrity			3	High	9
	ase any data reaks.			Rel	lative risl	x score:	l	16
				Tot	tal Risk S	core (Rel	x likelihood):	32

Risk Mitigation	R1 – Jami	ning	ultrasonic	sense	ors					
Choose action to take.	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	ţ		
Perception	Noise detecti	Noise detection and rejection Low								
Perception	Multiple sens	sors fo	r redundancy	check		Low	7			

Allegi	ro – Worksheet 10	R2 -	- <b>S</b> ]	poofing	ultrasonic	sensors				
	Business Asset	Ultra	son	ic sensors	data					
	<b>Business Asset's Value</b>	Low	– L	osing ultra	sonic sensors	data does n	ot impact BC	LT AV		
	Area of Concern	mani	pula	ate the da	trasonic freq ta received b the sensors a	y the sensor	rs causing fa	alse infor-		
	Actor Who would exploit the area of concern or threat?				ome previous nic emitter.	experience v	vith ultrasoun	d sensors.		
eat	Means How would the actor do it? What would they do?	An attacker uses their knowledge and tools to carry out a spoofin attack on ultrasonic ranging sensors by emitting carefully crafte frequencies and sequences causing false information received by th sensor.								
Threat	Motive What is the actor's reason for doing it?			•	AV program t	o keep drive	rs' jobs.			
	Outcome (choose one) What would be the resulting	D	)isc	losure:		Destruction:				
	effect be?	Mo	odi	fication:	X	Interr	ruption:			
	Security Requirements How would the information asset's security requirements be breached?	Ultra	son	ic sensors	are not spoof	ing resistant.				
	Likelihood (choose one)	Higl	h:		Medium	: x	Low:			
What a	equences  are the consequences to the organ  a result of the risk?	iza-	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			pact area	1 7	Priority*	Impact	Score		
harm to Not hav	o other road users. ving the sensor available without	any	Coı	nfidentiali	у	1	Low	1		
	ions will cause the system to not		Ava	ailability		2	High	6		
Spoofin	side, possibly other sensors can co ng attack on ultrasonic sensor will ny data leaks.	ver.		egrity		3	High	9		
	•			]	Relative ris	k score:		16		
		<b>Total Risk Score</b> (Rel x likelihood):						32		

Risk Mitigation	R2 – Spoo	fing ι	ıltrasonic	senso	ors					
Choose action to take.	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 detecti	on and	rejection			Low	7			
Perception	Multiple sens	Multiple sensors for redundancy check Low								

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?  Consequences  What would the information asset's security requirements be breached?  Likelihood (choose one) Likelihood (choose one)  Acoustic quieting will hide some objects from the ultrasonic ranging device. Not seeing possible obstacles can cause traffic accust and annot 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 as some objects are hidden.  No data leaks will be caused by 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.  No data leaks will be caused by 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.  No data leaks will be caused by 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.  No data leaks will be caused by 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.  No data leaks will be caused by 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.  No data leaks will be caused by 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.  No data leaks will be caused by 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  Total Ri	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 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) 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?  Acoustic quieting will hide some objects 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:  An attacker uses sound absorbing materials to cover some objects to make them harder to detect with ultrasound sensors. Has sound absorbing materials to use.  An attacker uses sound absorbing integrity of measurement data.  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 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.  Wattacker uses their knowledge and materials to cover nearby objects to make them harder to detect with ultrasound sensors which causes their knowledge and materials to ever nearby objects to make them harder to detect with ultrasound sensors which causes		<b>Business Asset</b>	Ultra	asonic se	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?  Motive  What would be the resulting effect be?  Modification:  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 is detected as some objects are hidden.  Relative risk score:  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 which causes their knowledge and materials to cover nearby objects to make them harder to detect with ultrasound sensors which causes their knowledge and materials to cover nearby objects to make them harder to detect with ultrasound sensors which causes their knowledge and materials to cover nearby objects to make them harder to detect with ultrasound sensors which causes have been caused them harder to detect with ultrasound sensors which causes have been caused them harder to detect with ultrasound sensors which causes have been caused them harder to detect with ultrasound sensors which causes have been caused them harder to detect with ultrasound sensors which causes		<b>Business Asset's Value</b>	Low	– Losir	ıg ultras	onic sensors	data does no	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	attacker	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	jects to make them harder to detect with ultrasound sensors							
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	nts 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:		Destr	ruction:			
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	lodifica	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	Ultra	asonic se	ensors a	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	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	t		
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		
					Rel	ative risk	score:	<u> </u>	12		

Risk Mitigation	R3 – Acoustic	quieting				
Choose action to take.	Accept:	Defer:	Mitigate:	X	Transfer:	
For the risk, what actions	and controls wil	ll be used:				
Layer where applied	Description of	control or ac	ction	Esti	imated cost	ţ
Perception	Multiple sensors for	or redundancy cl	heck	Low	r	

Allegr	ro – Worksheet 10	R4	– Ja	mmin	ıg r	adar				
	<b>Business Asset</b>	Suri	oundi	ng env	iron	ment data				
	<b>Business Asset's Value</b>	High	h - W	ithout S	Surr	ounding env	vironment 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?	An attacker with some previous experience with radars and has sig nal generator (+multiplier etc.).								
at	Means How would the actor do it? What would they do?	attac ing	ck on r false i	radar b	y en atio	nitting frequent	encies used b	to carry out a by the sensors nanging) rece	and caus-	
Threat	doing it?			rupt th	e A'		o keep drive			
	Outcome (choose one) What would be the resulting	Disclosure:			•		Destruction:			
	effect be?	M	Modification		n:		Interr	uption:	X	
	Security Requirements  How would the information asset's security requirements be breached?	Rad	ars are	e not ja	mm	ing resistan	t.			
	<b>Likelihood</b> (choose one)	Hig	gh:			Medium:	X	Low:		
What as	equences re the consequences to the organ a result of the risk? the integrity of data will cause the		How owne *3 fo	er by in	npac est p	ct area?		e organization ad 1 for lowes Impact		
tem to	make wrong decisions and poten other road users.	ntial	•	fidentia			1	Low	1	
	ving the sensor available without ons will cause the system to not									
the outs	ne outside, possibly other sensors can coamming attack on radar will not cause ata leaks.			ilability grity	/		2	High High	6	
					Re	elative ris	k score:		16	
				i	To	otal Risk S	Score (Rel	x likelihood):	32	

Risk Mitigation	R4 – Jammin	g radar								
Choose action to take.	Accept:	Defer:		Mitigate:	X	Transfer:				
For the risk, what actions and controls will be used:										
Layer where applied	<b>Description o</b>	of control or	actio	n	Est	imated cost	,			
Perception	Noise detection a	Noise detection and rejection Low								
Perception	Multiple sensors	for redundancy	check		Low	,				

Allegr	ro – Worksheet 10	R5	- Spoot	ing r	adar				
	<b>Business Asset</b>	Suri	rounding 6	nviror	ment data				
	<b>Business Asset's Value</b>	Hig	h – Witho	ut Suri	ounding env	rironment da	ta, car canno	t continue	
	Area of Concern	rada	r causing	consta		n distance/ve	ne data receivelocity on the data.		
	Actor Who would exploit the area of concern or threat?	An	attacker w	ith sor			vith radars an	d has sig-	
at	Means How would the actor do it? What would they do?	ing false information (no objects detected) received (76-77GH the experiment)							
Threat	Motive What is the actor's reason for doing it?	Waı	nts disrupt	the A	V program to				
	Outcome (choose one) What would be the resulting	]	Disclosu	re:		Destr	uction:		
	effect be?		Iodificat	ion:		Interr	uption:	X	
	Security Requirements  How would the information asset's security requirements be breached?	Rad	ars are no	t spoof	ing 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 b	ere are v impa	ct area?	r medium ar	e organizatio		
	the integrity of data will cause the make wrong decisions and poten		Impact a	rea		Priority*	Impact	Score	
Not hav	other road users.		Confide	ntiality		1	Low	1	
	ons will cause the system to not		Availabi			2	High	6	
	ide, possibly other sensors can co g attack on radar will not cause ks.		Integrity			3	High	9	
				R	elative ris	k score:		16	
				Te	otal Risk S	Score (Rel	x likelihood):	32	

<b>Risk Mitigation</b>	R5 – Spoo	fing r	adar						
Choose action to take.	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 detecti	Noise detection and rejection Low							
Perception	Multiple sens	Iultiple sensors for redundancy check Low							

Allegr	ro – Worksheet 10	<b>R6</b>	– Bli	inding at	tack on c	ameras			
	<b>Business Asset</b>	vide	o and	image data	a				
	<b>Business Asset's Value</b>		lium – ic ligh		continue dri	ving but car	i't recognize	signs and	
	Area of Concern	cam	era ca	using unw		ess, possible	ous optical d e hardware da		
	Actor Who would exploit the area of concern or threat?				me previous (laser etc.).	experience	and tools to s	end mali-	
at	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.							
Threat	Motive What is the actor's reason for doing it?	Wan	nts dis	rupt the A	V program t	o keep drive	rs' jobs.		
	Outcome (choose one) What would be the resulting	Ι	Discl	osure:		Destruction:			
	effect be?	M	Modification:		Interr	ruption:	X		
	Security Requirements  How would the information asset's security requirements be breached?	Cam	neras a	are vulnera	ble to blindi	ng 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 impao or highest p	ct area?	r medium ar	e organizatio 1d 1 for lowes		
	g attack will cause some blind sprage recorded by the cameras. B		Impa	act area		Priority*	Impact	Score	
sible ac	an cause not detecting objects and poisons because of that.		Conf	fidentiality		1	Low	1	
	ving the sensor available without					3	High	9	
the outs Using 1	ons will cause the system to not side, possibly other sensors can co asers to carry out the attack can	ver.	Integ	grity		2	High	6	
manent	ly damage the camera's lens	ļ		ים	_4!1			1.0	
					ative risk			16	
		<b>Total Risk Score</b> (Rel x likelihood):						48	

Risk Mitigation	R6 – Blinding	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	f control or a	ction	Est	imated cost				
Perception	Overlapping imag	Overlapping image output with multiple cameras Low							
Perception	Filter to remove h	narmful light		High	1				

Allegr	o – Worksheet 10	<b>R7</b>	<ul><li>Confus</li></ul>	ing o	controls v	vith attacl	k on came	ras		
	<b>Business Asset</b>	Vide	eo and Imag	e data	a					
	<b>Business Asset's Value</b>		lium – Car ic lights	can c	ontinue driv	ing but can	't recognize	signs and		
	Area of Concern						us optical sh			
		and blind cameras causing unwanted blindness and confusion fo longer period, possible hardware damage and loss of integrity o								
			eo and image			damage a	110 1088 01 11	neginy of		
	Actor						1. 1.	1 1'		
	Who would exploit the area of concern or threat?	ciou	s optical inp	outs (l	aser etc.), to	ools to furthe	and tools to ser destabilize	the input.		
	Means	An attacker uses their knowledge and malicious optical emitters to send a short output and blind cameras causing unwanted blindness								
ıt	How would the actor do it?						ng unwanted as and possib			
rea	What would they do?				mera sensor		as and possic	ny perma-		
Threat	Motive				program to		rs' jobs.			
•	What is the actor's reason for									
	doing it?	т	Disclosure		1	Doct	uction:			
	<b>Outcome</b> (choose one)  What would be the resulting	1	Disclosure	•		Desti	uction.			
	effect be?		Iodificatio	n·		Interruption:		X		
		141								
	Security Requirements									
	How would the information	Can	neras are vul	lnerah	ole to blindi	ng attacks.				
	asset's security requirements be breached?					-6				
	<b>Likelihood</b> (choose one)	Hig	vh·		Medium:	X	Low:			
	·	1112			Wicuiuii.	Λ	Low.			
	<b>quences</b> re the consequences to the organ	iza	Severity		the consequ	ioneos to thi	e organizatio	n or asset		
	a result of the risk?	ιζ.α-	owner by i			iences io inc	e organizano	n or ussei		
						· medium an	nd 1 for lowe:	st		
	g attack will cause some blind sp		Impact are	a		Priority*	Impact	Score		
	mage recorded by the cameras. B n cause not detecting objects and p		C	-1:4		1	T	1		
	cidents because of that. The blinds		Confidenti	anty		1	Low	1		
	r longer as the input is optimized.		Availabilit	V		3	High	9		
	ring the sensor available without		Integrity			2	High	6		
	ons will cause the system to not						-			
	ide, possibly other sensors can co asers to carry out the attack can									
	y damage the camera's lens.									
				Re	lative risl	score:		16		
				To	tal Risk S	core (Rel	c likelihood):	32		

Risk Mitigation	R7 – Confusin	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	<b>Description of</b>	control or ac	tion	Est	imated cost					
Perception	Perception Overlapping image output with multiple cameras Low									
Perception	Filter to remove ha	Filter to remove harmful light								

Allegi	ro – Worksheet 10	R8	– <b>R</b>	elay	attac	k on LiD	AR		
	<b>Business Asset</b>	Surr	ounc	ling ei	nviron	ment data			
	<b>Business Asset's Value</b>	Higl	h – V	Vithou	t Surre	ounding env	ironment da	ıta, car canno	t continue
	Area of Concern	the i	infor	mation usion,	ı got b	y the LIDA	R to carry or	wave and ma it the relay at f surrounding	tack caus-
	Actor Who would exploit the area of concern or threat?	with	spe	cific (9	905nm	) wavelengt	ths, oscilloso	•	C
sat	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							
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	Destruction:		
	effect be?	Modification:		on:	X	Interruption:			
	Security Requirements  How would the information asset's security requirements be breached?	LID	AR's	are n	ot rela	y attack res	istant.		
	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	re are impac	et area?		e organizatio	
	attack will manipulate with the d by the LiDAR. This causes error		Imp	oact ar	ea		Priority*	Impact	Score
fic.	tem and possible accidents in the		Coı	nfiden	tiality		1	Low	1
	lled errors can cause shutdown of	the	Ava	ailabil	ity		3	High	6
LiDAR Confide	 entiality is unaffected.		Inte	egrity			3 High		9
	· <b>y</b>				Rela	ative risk	score:	l	16
							core (Rel x	likelihood):	16

Risk Mitigation	R8 – Relay	y atta	ck on LiD	AR				
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			Higl	า	
Perception	Random probing Low							
Perception	Shorten pulse	e perio	d			Low	1	

Allegr	ro – Worksheet 10	R9 -	- Spoo	fing Li	iDAR			
	<b>Business Asset</b>	surro	unding 6	environr	nent data			
	<b>Business Asset's Value</b>	High	-Witho	out Surro	ounding env	ironment da	ta, car cannot	continue
	Area of Concern	DAR	in the	environn		e not there	o create object and causing l	
	Actor Who would exploit the area of concern or threat?				ne previous ) wavelengt		and tools to scope.	send light
<b>1</b>	Means How would the actor do it? What would they do?	An attacker uses their knowledge and tools to create objects for LI-DAR in the environment, that are not there.						
Threat	Motive What is the actor's reason for doing it?	Wan	ts disrup	t the AV	program to	keep drive	rs' jobs.	
	Outcome (choose one) What would be the resulting	Г	Disclosu	ıre:		Destr	uction:	
	effect be?	M	odifica	tion:		Interruption:		X
	Security Requirements  How would the information asset's security requirements be breached?	LIDA	AR's are	not spoo	ofing resista	nt.		
	Likelihood (choose one)	Hig	h:		Medium:		Low:	X
What a	equences re the consequences to the organ a result of the risk?	iza-	owner b	vere are vy impac	t area?		e organization	
	g artificial objects seen by the LiD use unwanted errors in the system.		Impact	area		Priority*	Impact	Score
interrup	management and could lead to tractions and accidents.		Confide	ntiality		1	Low	1
	on availability is there, but the att		Availab			2	Medium	4
new art	of remove real objects and only a ificial ones. entiality is not affected.	adds	Integrity	у		3	High	9
1	•	1		Re	lative risl	k score:		14
							x likelihood):	14

Risk Mitigation	R9 – Spoot	fing LiDAR								
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 control or ac	tion	Est	imated cost	t				
Perception	Multiple LiD	AR inputs		High	n					
Perception	Random prob	andom probing Low								
Perception	Shorton pulso	Shorten pulse period Low								

Allegi	ro – Worksheet 10	R10	) – (	Code n	nod	ification			
	<b>Business Asset</b>	syste	em so	oftware					
	<b>Business Asset's Value</b>	High	1 – sc	oftware	is res	sponsible fo	or controlling	g the car	
	Area of Concern		antec	d change				ne system codo oss of integrit	
	Actor Who would exploit the area of concern or threat?							vith car diagno e system code	
<b>t</b>	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.							
Threat	Outcome (choose one)		Wants disrupt the AV program to keep drivers'					rs' jobs.	
	What would be the resulting	Disclosure:			Destr	uction:			
	effect be?	Modification: x					Interr	uption:	
	Security Requirements  How would the information asset's security requirements be breached?	Syste	System software can be modified, no validation.						
	Likelihood (choose one)	Hig	h:			Medium:		Low:	X
What a	equences re the consequences to the organ a result of the risk?	iza-	Hov own	ner by in	прас	t area?		e organizatior	
	ring the code will cause unwanted d can possibly be used to harm the			act area			Priority*	Impact	Score
Depend	other road users. pending on the modified code, it can b		Con	ıfidentia	lity		1	Medium	2
	tem making it unavailable to use.		Ava	ilability	7		3	High	9
	the tools will allow the attacker to e used in the system.	see	Inte	grity			2	High	6
	* * * <b>/</b> **** *				Re	lative ris	k score:		17
				ļ	Total Risk Score (Rel x likelihood):				17

Risk Mitigation	<b>R10 – Cod</b>	le mo	dification							
Choose action to take.	Accept:									
For the risk, what actions	and controls will be used:									
Layer where applied	Description	Description of control or action Estimated cost								
Application	Device authe	nticati	on			Med	ium			
Application	Anti-malwar	Anti-malware Low								
Application	Isolation									

Allegr	o – Worksheet 10	R1	1 – Code	inje	ction				
	<b>Business Asset</b>	syst	em softwa	re					
	<b>Business Asset's Value</b>					or controlling			
	Area of Concern	caus		ited ch			code the sys n with loss of		
	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?	An attacker uses their knowledge and tools to inject code in the system causing unwanted changes and potential harm.							
Threat	Motive What is the actor's reason for doing it? Outcome (choose one)		nts disrupt	the AV	program to	o keep drive	rs' jobs.		
			Disclosur	e:		Destr	Destruction:		
			Iodificati	ification: x		Interr	uption:		
	Security Requirements  How would the information asset's security requirements be breached?	Har	mful code	can be	injected int	o system soi	ftware, no val	idation.	
	Likelihood (choose one)	Hig	gh:		Medium:		Low:	X	
What ar	<b>quences</b> re the consequences to the organ a result of the risk?	iza-	owner by	ere are impac	rt 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	he cars. All this impacts the busin also harm other road users when the move.		Integrity			3	High	9	
15 31		Relative risk score:					18		

Risk Mitigation	R11 – Cod	le inj	ection						
Choose action to take.	Accept:								
For the risk, what actions	and controls will be used:								
Layer where applied	Description of control or action								
Application	Device authe	nticati	on			Med	lium		
Application	Anti-malwar	Anti-malware Low							
Application	Isolation								

Allegr	o – Worksheet 10	<b>R</b> 1	2 – Packet	sn	iffing			
	<b>Business Asset</b>	Con	nmunication	data	ì			
	<b>Business Asset's Value</b>	Hig	h - without c	omr	nunication th	ne componer	nts can't work	together
	Area of Concern	com		in t	he system ca		and collect of confidential	
	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	nts to gather	clas	sified data to	sell to com	petitors.	
	Outcome (choose one) What would be the resulting	]	Disclosure	:	X	Destr	uction:	
	effect be?	M	Iodification	n:		Interr	uption:	
	Security Requirements  How would the information asset's security requirements be breached?	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		J.	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			Availability	y		1	Low	1
terruption	rectly installed sniffer won't cause a uptions in the communications and ity is not affected.		Integrity			2	Low	2
	sniffing does not affect the integrit munication (data will still be the sariginal).							
	<i>U /:</i>		1	R	elative risl	score:		12
				_			likelihood):	24

Risk Mitigation	R12 – Pac	ket sı	niffing					
Choose action to take.	Accept:		Defer:		Mitigate:	X	Transfer:	
For the risk, what actions and controls will be used:								
Layer where applied	Descriptio	n of o	control or	actio	n	Est	imated cost	
Communication	Encryption					Med	lium	
Communication	Device authentication Medium							
Communication	User authent	User authentication Medium						

Allegi	ro – Worksheet 10	<b>R</b> 1	3 – ]	Pack	et fuz	zing			
	<b>Business Asset</b>	Con	nmur	nicatio	n data				
	<b>Business Asset's Value</b>	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?		An attacker uses their experience to send invalid data to the system causing unwanted errors and potentially exposing security loopholes						
Threat	Motive What is the actor's reason for doing it?	Wai	Wants to find loopholes and cause errors in the vehicle.						
	Outcome (choose one) What would be the resulting			closure: Destructi				ruction:	
	effect be?	Modification: x Interruption:							
	Security Requirements How would the information asset's security requirements be breached?	Syst	tem o	an't h	andle	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 owi	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	Coı	nfiden	tiality		3	High	9
	anipulating the vehicle to attac	kers	Ava	ailabil	ity		1 Medium		2
control			Inte	grity			2	4	
		Relative risk score:					15		
		Total Risk Score (Rel x likelihood):						15	

Risk Mitigation	R13 – Pack	R13 – Packet fuzzing								
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								
Communication	Encryption			Higl	h					
Communication	Device authentication Medium									
Communication	User authentic	User authentication Medium								

Allegr	ro – Worksheet 10	R14	-Eave	sdrop	ping CAN	1			
	<b>Business Asset</b>	Com	municati	on data					
	<b>Business Asset's Value</b>	High	- withou	t comm	unication th	ne componer	nts can't wor	k together	
	Area of Concern	gaini	ing access	s to con		data and ca	to listen to using the loss		
	Actor Who would exploit the area of concern or threat?		<u> </u>				n to CAN bus	messages	
ı,	Means How would the actor do it? What would they do?				ir tools and		to listen to	CAN bus	
Threat	Motive What is the actor's reason for doing it?	Wan	ts to gath	er class	ified data to	sell to com	petitors.		
	Outcome (choose one) What would be the resulting		Disclosu	re:	X	Destr	uction:		
	effect be?	Modification:				Interr	uption:		
	Security Requirements  How would the information asset's security requirements be breached?	CAN bus can be listened to by outsiders							
	Likelihood (choose one)	Hig	h:		Medium:		Low:	X	
What a	equences re the consequences to the organ a result of the risk?	niza-	owner b	ere are v impac	t area?		e organizatio		
	ng to CAN messages can reveal coinformation to outsiders. The im-		Impact a	rea		Priority*	Impact	Score	
	less (but still high) than listenin communication as CAN is only		Confide	ntiality		3	High	9	
	of many different ones.	.	Availabi	lity		1	Low	1	
terruption ability	ly installed sniffer won't cause any ons in the communications and av- is not affected nor is the integrity sages should not be modified to av-	vail- y as	Integrity			2	Low	2	
1111011115		Relative risk score:						12	
							likelihood):	12	
				<b>Total Risk Score</b> (Rel x likelihood):					

Risk Mitigation	R14 -Eave	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	Descriptio	Description of control or action									
Communication	Encryption					High	n				
Communication	Device authentication Medium										
Communication	User authentication Medium										

Allegr	o – Worksheet 10	R15	5— I	nject (	CAN	N message	es		
	<b>Business Asset</b>			nication					
	<b>Business Asset's Value</b>	High	1 - W	ithout co	omm	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	attac]	ker with	tool	s to inject C	CAN messag	es.	
<b>+</b>	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.						
Threat	Motive What is the actor's reason for doing it?	Wan	ıts di	srupt the	e AV	program to	keep drive	rs' jobs.	
	Outcome (choose one) What would be the resulting	I	Disc	losure:	e: x		Destr	ruction:	
	effect be?	Modification: Interruption:							
	Security Requirements  How would the information asset's security requirements be breached?	No a	uthe	enticatio	n for	· CAN mess	ages.		
	Likelihood (choose one)	Hig	gh:			Medium:		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	messages cause wrong decisions by dri planner and harm to the vehicle or passer			nfidentia	lity		2	Medium	4
is possil		. [	Ava	ailability	7		1	Medium	2
	ssages can be used to shut down components.	1m-	Inte	grity			3	High	9
					Re	lative ris	k score:		15
					Total Risk Score (Rel x likelihood):				

Risk Mitigation	R15– Inje	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	Descriptio	Description of control or action									
Communication	Encryption					High	า				
Communication	Device authe	Device authentication Medium									
Communication	User authentication Medium										

Allegi	ro – Worksheet 10	R1	6 – <b>GPS</b>	jamr	ning and	spoofing			
	<b>Business Asset</b>	Loc	ation data						
	<b>Business Asset's Value</b>				location is e				
	Area of Concern	GPS	S, making t	the vel			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 jam the GPS, making the vehicle localization not possible.						
Threat	Motive What is the actor's reason for doing it?	Waı	nts disrupt	the AV	V program to	keep drive	rs' jobs.		
	Outcome (choose one) What would be the resulting		Disclosure: Destruction:						
	effect be?	Modification: Interruption:						X	
	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	Low:		
What a	equences re the consequences to the organ a result of the risk?	iza-	owner by	ere 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	
			1	Rela	ative risk	score:	l	16	
					al Risk So		likelihood):	32	

Risk Mitigation	R16 – GPS ja	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	Description of	f control or	actio	n	Est	imated cost				
Perception	Perception Nullification High									
Perception	Monitoring signa	Monitoring signals and identification nodes Medium								

Allegr	o – Worksheet 10	R1	7 – EMP a	ittac	eks				
	<b>Business Asset</b>	Aut	onomous dri	ving					
	<b>Business Asset's Value</b>		h – Without						
	Area of Concern	AV,		onom	ous driving	impossible	wn componer and causing t		
	Actor Who would exploit the area of concern or threat?		attacker with						
ıt l	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.						
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 effect be?		Disclosure:			Destr	ruction:		
			Modification: Interru				ruption:	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)	Hig	gh:		Medium:		Low:	X	
What ar	quences re the consequences to the organ a result of the risk?	iza-	owner by in	npac	t area?		e organization		
	tacks can shut down component Depending on the pulse genera		Impact area	ı		Priority*	Impact	Score	
affect ve	act is different. Small pulse may carry small components but bigger of	ones	Confidentia	ality		1	Low	1	
	ct larger components and even ca		Availability	y		3	High	9	
	ent damage. Generating high important shard and the tools used are exp		Integrity			2	Low	2	
				Re	lative risk	score:		12	
				To	tal Risk S	core (Rel	x likelihood):	12	

Risk Mitigation	R17 – EM	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 Medium									

Allegr	ro – Worksheet 10	R1	8 – Injec	t ma	lware			
	<b>Business Asset</b>	Aut	onomous d	lriving				
	<b>Business Asset's Value</b>	Hig	h – Withou	ıt auto	nomous driv	ing, it is a n	ormal car	
	Area of Concern	syst		g erro	rs, loss of d		inject malwar ts and loss of	
	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.
it.	Means How would the actor do it? What would they do?	An attacker uses physical ports or network to inject malware into the system.						
Threat	Motive What is the actor's reason for doing it?		Depending on the malware, the attacker can gather classifi disturb the processes and so on.					
	Outcome (choose one) What would be the resulting	]	Disclosure: Destruction:				X	
	effect be?		Iodificati	on:		Interr	uption:	
	Security Requirements  How would the information asset's security requirements be breached?	Phy	sical port o	or netv	vork can be	used to injec	t 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	lriv-	Confiden	tiality		3	High	9
	cess, causing harm to the component	ents	Availabil	ity		2	High	6
	on.  outcome is the destruction of the us driving process.	au-	Integrity	-		1	High	3
	<u> </u>			Rela	ative risk	score:		18
				Tot	ol Dielz Se	core (Rel x	likalika ad).	36

Risk Mitigation	R18 – Inje	R18 – Inject malware									
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, communication	Install firewa	11				Low	7				
Application	Anti-malware Low										
Application	Isolation Medium										

Allegi	ro – Worksheet 10	R19	<b>)</b> _ ]	Manipula	te map da	ıta			
	<b>Business Asset</b>	Map	data	a					
	<b>Business Asset's Value</b>	High	1 – N	Aap is requi	red 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.		
<del>1</del>	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?								
	Outcome (choose one) What would be the resulting	Γ	Disc	losure:		Destr	Destruction:		
	effect be?	M	odi	fication:	Х	Interr	ruption:		
	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?	viza-	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	reet	Coı	nfidentiality		2	Low	2	
hit obje			Ava	ailability		1	Low	1	
			Inte	egrity		3	High	9	
				Rela	ative risk	score:		12	
				Tot	al Risk So	core (Rel x	likelihood):	12	

Risk Mitigation	R19 – Mai	R19 – Manipulate map data								
Choose action to take.	Accept:	De	efer:		Mitigate:	X	Transfer:			
For the risk, what actions and controls will be used:										
Layer where applied	Descriptio	Description of control or action								
Application	Isolation					Med	ium			
Application	Device authe	Device authentication Medium								
Application	User authenti	User authentication Medium								

Allegi	ro – Worksheet 10	R20	0 – 1	Extract m	ap data				
	<b>Business Asset</b>	Map	data	ı					
	<b>Business Asset's Value</b>	Higl	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	attacl	ker with acc	ess to the st	orage and m	aps.		
	Means How would the actor do it? What would they do?			ker uses the ion leak.	ir access to	the maps to	extract then	n, causing	
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: x			Destr	Destruction:			
		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	equences re the consequences to the organ a result of the risk?	iza-	Ho	ner by impa	ct area?		e organizatio		
	g access to the map data will cause risks in other aspects. Knowing v		_	oact area	priority, 2 fa	Priority*	nd 1 for lowes Impact	Score	
lines an	d what streets will most likely be used by the attacker to prepare o	ısed	Cor	nfidentiality		3	High	9	
attacks.			Ava	ailability		1	Low	1	
Selling	elling of the data is possible.			egrity		2	Low	2	
				Rel	ative risk	score:		12	
				Tot	al Risk S	core (Rel x	likelihood):	12	

Risk Mitigation	<b>R20</b> – <b>Ext</b>	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	applied Description of control or action Estimated cost										
Application	Isolation					Med	ium				
Application	Device authentication Medium										
Application	User authent	User authentication Medium									

Allegi	ro – Worksheet 10	R21	l – ]	Delete ma	p data			
	<b>Business Asset</b>	Map	data	a				
	<b>Business Asset's Value</b>	High	1 – N	Aap is requir	ed to know	where roads	are	
	Area of Concern		ic di				elete them, re of availabilit	
	Actor Who would exploit the area of concern or threat?	An a	ıttac	ker with acc	ess to the sto	orage and m	aps.	
<b>+</b> 2	Means How would the actor do it? What would they do?			ker uses thei sturbances a			elete them, re	esulting in
Threat	Motive What is the actor's reason for doing it?	Wants disrupt the AV			V program to	_		
	Outcome (choose one) What would be the resulting		Disc	losure:		Destruction:		X
	effect be?	Modification:			Interr			
	Security Requirements How would the information asset's security requirements be breached?	Storage and map data			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 impac	ct area?		e organizatio ud 1 for lowes	
	nta is crucial for autonomous drivering it will cause the vehicle to			pact area		Priority*	Impact	Score
and co	nd continuing the work is impossible ew data is provided.			nfidentiality		2	Low	2
			Ava	ailability		3	High	9
			Inte	egrity		1	Low	1
				Rela	ative risk	score:		12
				Tot	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 of control or action								
Application	Isolation			Medium					
Application	Device auther	Device authentication Medium							
Application	User authentic	User authentication Medium							

Allegr	ro – Worksheet 10	R22	2 – ]	Disabl	e ac	tuation n	odule		
	<b>Business Asset</b>	Auto	onon	nous dri	ving				
	<b>Business Asset's Value</b>	High	1 – V	Vithout	autor	nomous driv	ing, it is a n	ormal car	
	Area of Concern		ble tl					on module, will ability of auto	
	Actor Who would exploit the area of concern or threat?	An a	attac]	ker who	can	install malv	vare on the a	actuation modu	ıle.
it.	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.						
Threat	Motive What is the actor's reason for doing it?	Wan	ıts di	srupt th	e AV	<sup>7</sup> program to	keep drive	rs' jobs.	
	Outcome (choose one) What would be the resulting	Ι	Disc	losure	re:		Destruction:		
	effect be?	M	Modification:				Interr	ruption:	X
	Security Requirements How would the information asset's security requirements be breached?	Actuation modul			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?	iza-	Ho owr	ner by in	прас	t area?		e organization	
	on module is responsible to carry trols given by computing unit. W			act area			Priority*	Impact	Score
out it, a Disabli	nutonomous driving is impossible.  ng the actuation module can be u	ısed	Cor	nfidentia	ality		1	Low	1
to dema	and money for the malware remov	al.		ailability	у		3	High Medium	9
			Integrity				2	4	
						lative risl			14
					To	tal Risk S	Score (Rel :	14	

Risk Mitigation	R22 – Disa	R22 – Disable actuation module									
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	ontrol or	actio	n	Est	imated cost	t			
Application	v 11 1										
Application	Access Contro	ol				Low	7				

Allegi	ro – Worksheet 10	R2	3 – Ind	uce ba	d analysi	S			
	<b>Business Asset</b>	Aut	onomous	driving	-				
	<b>Business Asset's Value</b>	Hig	h – Witho	out auto	nomous driv	ing, it is a n	normal car		
	Area of Concern	war	e causing	the car	to follow a		fake output of ers and causin ner		
	Actor Who would exploit the area of concern or threat?	An	attacker v	vith kno	wledge on t	he used soft	ware.		
;	Means How would the actor do it? What would they do?		An attacker uses their knowledge to create fake output of the ware causing the car to follow attackers orders.						
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			
			Modification: x			Interr	ruption:		
	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?	niza-	owner b	vere are vy impac	rt area?		e organizatior		
	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.	Availability				2	Medium	4	
harm to	an attacker control the car can can the car itself, passengers or other and their property.		Integrit	у		3	High	9	
asers ar	na men property.	Relative risk score:						14	
						re (Rel x lil	kelihood):	14	
				I Juli	TAIDIN DCU	Le INEI A III	announ.		

Risk Mitigation	R23 – Indu	R23 – Induce bad analysis									
Choose action to take.	Accept:	X	Transfer:								
For the risk, what actions and controls will be used:											
Layer where applied	Description	Description of control or action Estimated cost									
Application	Isolation			Med	lium						
Application	Access Contr	Access Control Low									
Application	Input validati	nput validation Low									

## II. Validated OCTAVE Worksheets

Allegi	ro – Worksheet 10	R4	– Ja	mmin	g r	adar			
	<b>Business Asset</b>	Surr	ound	ing envi	ron	ment data			
	<b>Business Asset's Value</b>	Low	-Lo	sing rad	dar	data does n	ot impact B	OLT AV	
	Area of Concern	rada	r cau		se bl	lackout on th		ne data receive loss of integri	
	Actor Who would exploit the area of concern or threat?					ne previous of iplier etc.).	experience v	vith radars and	d has sig-
at	Means How would the actor do it? What would they do?	attac ing t	An attacker uses their knowledge and tools to carry out a jammin attack on radar by emitting frequencies used by the sensors and causing false information (distance constantly changing) received (7 77GHz in the experiment).						
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	Ι	Disclosure				Destruction:		
	effect be?		Modification:			Interr	ruption:	X	
	Security Requirements How would the information asset's security requirements be breached?	Rada	ars ar	e not ja	mm	ing resistant		1	
	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 own *3 fe	er by im or highe	ipac est p	ct area?	r medium ar	e organization	
	the integrity of data will cause the make wrong decisions and poter		Imp	act area			Priority*	Impact	Score
harm to Not hav	o other road users. ving the sensor available without	any	Con	fidentia	lity		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.		Inte	grity			2	High	6
		I			Re	elative ris	k score:		16
					To	tal Risk S	Score (Rel :	x likelihood):	32

Risk Mitigation	R4 – Jami	R4 – Jamming radar								
Choose action to take.	Accept:	Accept: Defer: Mitigate:								
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	V 11 1									
Perception	Multiple sens	sors for	r redundancy	check		Low	7			

Allegr	o – Worksheet 10	R5	- S <sub>1</sub>	poofin	g ra	adar			
	<b>Business Asset</b>	Suri	ound	ling env	iron	ment data			
	<b>Business Asset's Value</b>	Low	, – L	osing ra	dar	data does n	ot impact Be	OLT AV	
	Area of Concern	rada	ır cau	sing co	nsta	nt changes in		e data receiv locity on the data.	
	Actor Who would exploit the area of concern or threat?	An a	attacl	cer with	son			vith radars an	d has sig-
at	Means How would the actor do it? What would they do?	attac ing	ck on false	radar b	y en	nitting freque	encies used b	o carry out a y the sensors eceived (76-	and caus-
Threat	Motive What is the actor's reason for doing it?	War	nts di	srupt th		V program t	o keep drive	rs' jobs.	
	Outcome (choose one) What would be the resulting	Disclosure			•		Destr	uction:	
	effect be?	M	Modification:				Interr	uption:	X
	How would the information asset's security requirements be breached?	Rad	ars a	re not sp	oof	ing resistant	i.		
	Likelihood (choose one)	Hig	gh:			Medium:	X	Low:	
What ar	quences re the consequences to the organ result of the risk?	iza-	Hov owr	ier by ir	прав	ct area?		e organization	
	he integrity of data will cause the make wrong decisions and poter		Imp	act area	ı		Priority*	Impact	Score
Not hav	other road users. ring the radar available without		Cor	nfidentia	lity		1	Low	1
	ons will cause the system to not			/		2	High	6	
	ide, possibly other sensors can cog attack on radar will not cause ks.		Inte	grity			3	High	9
					Re	elative ris	k score:		16
		Total Risk				otal Risk S	Score (Rel x	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	Descriptio	n of c	control or	actio	n	Est	imated cost	;		
Perception	Noise detecti	Noise detection and rejection Low								
Perception	Multiple sensors for redundancy check Low									

Allegr	ro – Worksheet 10	<b>R7</b>	– Confusi	ing (	controls v	with attac	k on came	ras
	<b>Business Asset</b>	Vid	eo and Imago	e data	a			
	<b>Business Asset's Value</b>	Hig	h – Image re	ecogi	nition is ess	ential for sa	fe driving	
	Area of Concern	and long	blind camer	ras ca ossib	ausing unw ole hardwar	anted blindr	us optical shoness and confind loss of in	fusion 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?	seno	An attacker uses their knowledge and malicious optical emitters send a short output and blind cameras causing unwanted blindness confusion for longer period and messing with auto exposure on to cameras and possibly permanently damage the camera sensors.					
Threat	Motive What is the actor's reason for doing it?	Mes	ss with imag	e rec	ognition to	cause accid	ents.	
	Outcome (choose one) What would be the resulting	]	Disclosure	:		Destr		
	effect be?	N	Iodification	n:		Interr	Interruption:	
	Security Requirements How would the information asset's security requirements be breached?	Can	neras are vul	ulnerable 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?	niza-	owner by in	трас	t area?		e organization	
	asers to carry out the attack can ly damage the camera's lens.	per-	Impact area	a		Priority*	Impact	Score
Messing	g with camera inputs and auto ex ill make it harder to detect tro	iffic	Confidentia	ality		1	Low	1
	signs and pedestrians. More likel	- Trumuomty				3	High	9
cause a	ccidents.		Integrity			2 High		6
					lative ris			16 48
		<u></u>			<b>Total Risk Score</b> (Rel x likelihood):			

Risk Mitigation	R7 – Conf	R7 – Confusing controls with 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	Description of control or action										
Perception	Overlapping	Overlapping image output with multiple cameras Low										
Perception	Turn off auto exposure Low											

Allegi	ro – Worksheet 10	R8	– <b>R</b>	elay attac	k on LiD	AR				
	<b>Business Asset</b>	Suri	rounc	ding environ	ment data					
	<b>Business Asset's Value</b>	Hig	h - V	Vithout Surr	ounding env	ironment da	ta, car canno	continue		
	Area of Concern	the ing	infor conf nt dat	mation got busion, errors	by the LIDA s and loss on the thing with the	R to carry ou f integrity o	vave and man at the relay at f surrounding aputs could po	ack caus-		
	Actor Who would exploit the area of concern or threat?	with	ı spe	cific (905nm	n) waveleng	ths, oscilloso	•			
Threat	Means How would the actor do it? What would they do?	con	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.							
Thi	Motive What is the actor's reason for doing it?	Wants disrupt the AV program				o keep drive	rs' jobs.			
	Outcome (choose one) What would be the resulting	]	Disclosure:			Destruction:				
	effect be?		Modification:			Interr	uption:			
	Security Requirements  How would the information asset's security requirements be breached?	LID	AR's	s are not rela	y attack res	sistant.				
	Likelihood (choose one)	Hig	gh:		Medium:		Low:	X		
What a	equences  tre the consequences to the organ  a result of the risk?	Severity  How severe are the consequences to the organization or asserowner by impact area?  *3 for highest priority, 2 for medium and 1 for lowest								
	ring LiDAR inputs in certain way I to control the car by an attacker			pact area	<i>y</i> , <i>y</i>	Priority*	Impact	Score		
		Confidentiality				1	Low	1		
		Availability			3	High	6			
		Integrity			3	9				
				Rela	ative risk	score:		16		
		<b>Total Risk Score</b> ( <i>Rel x likelihood</i> ): <b>16</b>								

<b>Risk Mitigation</b>	R8 – Rela	R8 – Relay attack on LiDAR									
Choose action to take.	Accept:	Accept: Defer: Mitigate: x Transfer:									
For the risk, what actions and controls will be used:											
Layer where applied	Description	Description of control or action									
Perception	Multiple LiD	Multiple LiDAR inputs High									

Allegi	ro – Worksheet 10	R9	$-\mathbf{S}$	poofin	g Li	DAR			
	<b>Business Asset</b>	surr	ound	ing env	ironn	nent data			
	<b>Business Asset's Value</b>	High	h-I	LiDAR i	s pri	mary tool fo	or obstacle d	letection	
	Area of Concern	DAI	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	spe	cific (90	)5nm		hs, oscilloso	and tools to scope.	send light
it.	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?	War	nts di	srupt th	e AV	<sup>7</sup> program to	keep drive	rs' jobs.	
	Outcome (choose one) What would be the resulting	Disclosure:		-		Destruction:			
	effect be?	Modification			n:		Interr	uption:	X
	Security Requirements How would the information asset's security requirements be breached?	LIDAR's are not			spoo	ofing resista	nt.		
Ì	Likelihood (choose one)	Hig	gh:	x		Medium:		Low:	
What a	equences re the consequences to the organ a result of the risk?	Severity  niza- 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							
	g smoke clouds will cause the detect them as obstacles. Detec			pact area			Priority*	Impact	Score
such si gency	uch smoke with LiDAR can cause en ency braking and possible accidents		Cor	nfidentia	ality		1	Low	1
cause o	ause of that.			Availability			2 Medium		4
			Inte	egrity			3	9	
				Relative risk score:				14	
		<b>Total Risk Score</b> (Rel x				: likelihood):	42		

Risk Mitigation	R9 – Spoofi	R9 – Spoofing LiDAR									
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											
Perception Multiple LiDAR inputs High											
Perception	Better obstacle detection algorithms Low										

Allegr	o – Worksheet 10	R1	0 – 0	Code 1	nod	ification				
	<b>Business Asset</b>	Syst	tem s	oftware						
	<b>Business Asset's Value</b>	Hig	h – s	oftware	is re	sponsible fo	or controlling	g the car		
	Area of Concern	unw	ante	d chang	es ar	nd potential	•	he system cod loss of integri ories.	_	
	Actor Who would exploit the area of concern or threat?	codi	ing c	an use (	OBD			vith car diagno ne system cod		
it.	Means How would the actor do it? What would they do?						ge and tools es and poten	to modify co	de in the	
Threat	Motive What is the actor's reason for doing it?	Waı	nts di	srupt th	ie AV	program to	keep drive	rs' jobs.		
	Outcome (choose one) What would be the resulting	Disclosure		:		Destruction:				
	effect be?	M	Modification		n:	X	Interr	ruption:		
	Security Requirements How would the information asset's security requirements be breached?	System software car				e can be modified, no validation.				
	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	mpac	rt area?		e organization		
	ng the code in the repository problems with all the cars using			pact area	_		Priority*	Impact	Score	
same co	ause problems with all the cars using ame code. Atacker can use the modified code to co		Coı	nfidentia	ality		1	Medium	2	
	the next person in the car.		Av	ailabilit	V		3	High	9	
	•			egrity	/	2 High		6		
L		Relative risk score:					17			
								x likelihood):	17	
		1 otal High Scote (het a timetino ot								

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	Unit tests					Low	t.				
Application	Regular manual checks Low										
Application	Access control Low										

Allegr	o – Worksheet 10	R1.	3 – ]	Packet fu	zzing				
	<b>Business Asset</b>	Con	nmur	nication data	ı				
	<b>Business Asset's Value</b>	High geth		without con	nmunication	the comp	onents can't	work to-	
	Area of Concern	and	pote	ntially expo		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?		An attacker uses their experience to send invalid data to the scausing unwanted errors and potentially exposing security loop						
Threat	Motive What is the actor's reason for doing it?	War	nts to	find loopho	oles and cause errors in the vehicle.				
	Outcome (choose one) What would be the resulting effect be?		Disc	losure:		Destruction:			
			lodi	fication:	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 ar	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 validation data will cause errors in		Imp	pact area		Priority*	Impact	Score	
system. loophol	system. The outcomes could be used to oopholes in the security for other attacl			nfidentiality		3	High	9	
	inipulating the vehicle to attack	kers	Ava	ailability		1	Medium	2	
control.		Integrity			2 Medium		4		
		Relative risk score:						15	
		Total Risk Score (Rel x likelihood): 15						15	

Risk Mitigation	R13 – Pac	R13 – Packet fuzzing									
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										
Communication	Encryption					High	h				
Communication	User authen	ticatio	n			Med	lium				
Communication	Secure connection Medium										
Communication	Split network (multiple smaller parts) Low										

Allegi	ro – Worksheet 10	R1	6 – 6	GPS jamı	ning						
	<b>Business Asset</b>	Location data									
	<b>Business Asset's Value</b>	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 GPS, making the vehicle localization not possible and cau loss of integrity of location data.  GPS also uses correction got in real-time which could be an opportunity.								
Threat	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?	Wai	nts di	srupt the A	V program to	rogram to keep drivers' jobs.					
	Outcome (choose one) What would be the resulting		Disc	losure:		Destr					
	effect be?	M	Iodi	fication:		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 organ tion as a result of the risk?		niza-	iza- How severe are the consequences to the organization of 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 poter		sys- Impact area			Priority*	Impact	Score			
harm to other road users.  The correction is used to get even less er			Confidentiality			1	Low	1			
(from meters to few centimetres), mess			Ava	ailability		3	High	9			
with it can cause accidents on the road.			Integrity			2	High	6			
		Relative risk score:						16			
		<b>Total Risk Score</b> (Rel x likelihood):						32			

Risk Mitigation	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	Duplicate GPS Medium								
Perception	Use LiDAR for localization Low								

Allegr	o – Worksheet 10	R1	7 – EMP a	atta	cks					
	<b>Business Asset</b>	Aut	onomous dri	ving						
	<b>Business Asset's Value</b>	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.							
Threat	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.							
	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:		Interr	ruption:	X		
	Security Requirements  How would the information asset's security requirements be breached?	Elec	etronic comp	oner	nts in AV ca	n be affected	d with EMP.			
	Likelihood (choose one)	Hig	gh:		Medium:		Low:	x		
Consequences What are the consequences to the organition as a result of the risk?			iza- How severe are the consequences to the organization or assowner by impact area? *3 for highest priority, 2 for medium and 1 for lowest							
EMP attacks can shut down components the car. Depending on the pulse generate the impact is different. Small pulse may or affect very small components but bigg			Impact area	a		Priority*	Impact	Score		
		only gger	Confidentia			1	Low	1		
ones can affect larger components and even			Availability			3	High	9		
cause permanent damage. Generating hi impact pulses is hard and the tools used a expensive.		high Integrity		-		2	Low	2		
			1	Re	elative ris	k score:	l	12		
							x likelihood):	12		

Risk Mitigation	R17 – EMP attacks								
Choose 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							ţ		

Allegi	ro – Worksheet 10	R19	9 – ]	Mani	ipulat	te map da	ıta				
	<b>Business Asset</b>	Map	data	a							
	<b>Business Asset's Value</b>	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 t 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. Possibly inside								
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.							m, result-		
	Motive What is the actor's reason for doing it?	Wants disrupt			rupt the AV program to keep drivers' jobs.						
	Outcome (choose one) What would be the resulting effect be?		Disclosure:				Destruction:				
			Modification:			X	Interr				
	Security Requirements How would the information asset's security requirements be breached?	Storage and m			I map data are not authenticated.						
	Likelihood (choose one)	Hig	igh:			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 of owner by impact area?  *3 for highest priority, 2 for medium and 1 for lowest								
	ata 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 hit objects.			treet Confidentiality				2	Low	2		
			Av	ailabil	ity	_	1 Low		1		
			Integrity				3 High		9		
		Relative risk score: Total Risk Score (Rel x li						12			
							likelihood): 12				

Risk Mitigation	R19 – Manipulate map data								
Choose action to take.	Accept:	Defer:	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 th	Low	,					