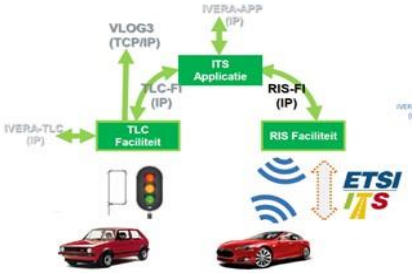
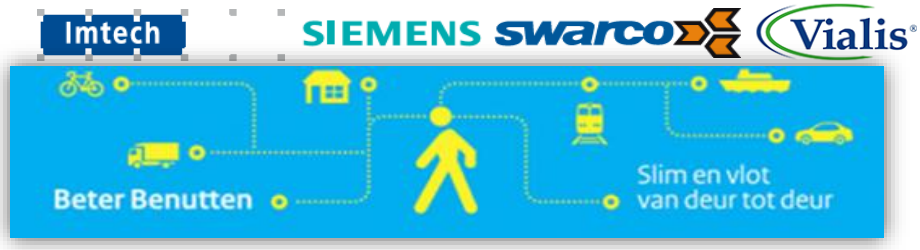
Intelligente Verkeers Regel Installatie (iVRI) – Fase 1

Deliverable H2: iVRI Security & Safety matrix

Security and Safety analysis





Datum: 27 januari 2016
Versie: 1.2

VOORWOORD

In juni 2015 is opdracht verstrekt door het Ministerie van Infrastructuur en Milieu via het Beter Benutten Vervolg (BBV) programma aan vier VRA leveranciers om te komen tot een gezamenlijke definitie van VRA standaarden ten behoeve van connected en coöperatieve functionaliteit.

Dit document vormt Deliverable H2 van de afgesproken leverdelen in de opdrachtverstrekking, omschreven als “Security & Safety Matrix”.

Deze deliverable beschrijft gedeeltelijk in het Engels de Security en Safety analyse van een iTLC.

Dit document is tot stand gekomen door samenwerking van de vier leveranciers in de werkgroep bestaande uit:

Inge Fløan

Hans Looijen

Peter Smit

Jeroen Hiddink

NB. De rest van dit document is gedeeltelijk geschreven in het Engels om internationale uitwisseling te ondersteunen.

The rest of this deliverable has been written partly in English to facilitate international exchange.

Introduction

This document contains a security matrix and safety matrix.
Each matrix contains threats, effects, impact, probability, measures and remaining risk.
It is the result of thorough analysis excecuted from the point of view of the stakeholders.

Stakeholders

Beter Benutten; funds the development of the interface descriptions and architecture to allow an open market
Road authorities; it is in their interest to be able to deploy iTLCs, independently of a manufacturer, but with standard interfaces and clearly defined behavior.

TLC manufacturers; who implements the defined architecture and standard interfaces into the various TLC products

RIS manufacturers; who implements the defined architecture and standard interfaces into the various RIS products
Application providers
Road users
Maintenance engineers
Traffic Engineers
Installation Engineer
Local ad-hoc Operator
Service Provider
Traffic Management System (incl. Operator)
Traffic Control System
Traffic Data Centre

iVRI Security matrix conform ISO27002

	Subject	Threats	Effect	Initial: Confidentiality	Integrity	Availability	Authenticity	Reliability	Impact	Probability	Risk	Measures				Remaining: Impact	Probability	Risk
General																		
	Security maatregelen	Onwerkbare situatie, dagelijkse workflow impact	Er worden bypasses verzonnen, om efficient te kunnen werken	X	X	X	X	X	5	3	15	Procedures op voorhand laten controleren	Onafhankelijk auditing process, met onafhankelijk proces voor de findings	Procedures zoveel mogelijk automatiseren door tooling		5	1	5
		Teveel/moeilijk maatregelen/procedures	Security wordt foutief geimplementeerd en is dus niet waterdicht	X	X	X	X	X	5	3	15	Automatisering van procedures en de implementatie van maatregelen	Maatregel en procedures op voorhand controleren op haalbaarheid	Continue verbeterproces voor de maatregelen		5	1	5
Human resource security																		
												Prior to employment	*During employment*	*Termination of employment*				
	Personen die rechtstreeks contact hebben met iTLC	Kunnen onbetrouwbaar *(wel bevoegd!)* zijn	De regeltoestand wordt negatief beinvloed De verkeersveiligheid wordt negatief beinvloed De security wordt afgezwakt of opengezet			X	X	X	5	2	10	Personeel screenen	Personeel controleren	Persoonlijke toegangsrechten en logins verwijderen, apparatuur innemen		5	1	5
		Kunnen onbekwaam *(wel bevoegd!)* zijn	De regeltoestand wordt negatief beinvloed De verkeersveiligheid wordt negatief beinvloed De security wordt afgezwakt of opengezet			X	X	X	3	3	9	Personeel met juiste opleidingsniveau	Personeel controleren en juiste opleiding geven	Persoonlijke toegangsrechten en logins verwijderen, apparatuur innemen		3	1	3
		Kunnen onbevoegd zijn	De regeltoestand wordt negatief beinvloed De security wordt afgezwakt of opengezet			X	X	X	3	2	6		Persoonlijke toegangsrechten en logins beheren	Persoonlijke toegangsrechten en logins verwijderen, apparatuur innemen		3	1	3
	Personen die via Applicaties (indirect) contact met iTLC	Kunnen onbetrouwbaar (*wel bevoegd!)* zijn	De regeltoestand wordt negatief beinvloed De verkeersveiligheid wordt negatief beinvloed De verkeerde LDM objecten worden aangemaakt (kan resulteren in ten onrechte verzonden ITS G5 messages) De functies van TLC-FI en RIS-FI worden misbruikt De IVERA toegang wordt misbruikt			X	X	X	5	2	10	Personeel screenen	Personeel controleren	Persoonlijke toegangsrechten en logins verwijderen en aanverwante apparatuur		5	1	5
		Kunnen onbekwaam *(wel bevoegd!)* zijn	De regeltoestand wordt negatief beinvloed De verkeersveiligheid wordt negatief beinvloed De verkeerde LDM objecten worden aangemaakt (kan resulteren in ten onrechte verzonden ITS G5 messages)			X	X	X	5	2	10	Personeel met juiste opleidingsniveau	Personeel controleren en juiste opleiding geven	Persoonlijke toegangsrechten en logins verwijderen en aanverwante apparatuur		5	1	5
		Kunnen onbevoegd zijn	De regeltoestand wordt negatief beinvloed De verkeersveiligheid wordt negatief beinvloed De verkeerde LDM objecten worden aangemaakt (kan resulteren in ten onrechte verzonden ITS G5 messages)			X	X	X	5	5	25		Persoonlijke toegangsrechten en logins beheren	Persoonlijke toegangsrechten en logins verwijderen en aanverwante apparatuur		5	1	5
Asset management																		
												Prior to installation	*During operation*	*After deinstallation*				
	Wegkant-apparatuur (routers, modem, TLC,)	Het RIS systeem wordt niet goed geinstalleerd	Er wordt foutieve informatie verstrekt aan C-ITS stations, daardoor wordt het verkeersonveilig voorbeeld: topology-informatie verspreid door RIS komt niet overeen met de werkelijke topology.			X	X		5	5	25	Controle, test en installatie richtlijnen opstellen	Controle en onderhoud uitvoeren op werking en procedures (audit) Self-audit of RIS; if something is wrong, take according action. E.g. transmit SPAT-unknown when TLC is offline	Security gegevens non-recoverable verwijderen		5	1	5
		De TLC wordt niet goed geinstalleerd	De verkeersregeling wordt niet goed afgewikkeld, of is zelfs verkeerd. De bedrading kan verkeerd worden aangesloten. Situatie op het kruispunt kan verkeersonveilig worden			X	X		5	2	10	Controle, test en installatie richtlijnen opstellen	Controle en onderhoud uitvoeren op werking en procedures (audit)	Security gegevens non-recoverable verwijderen		5	1	5
		De security-settings worden niet (correct) ingesteld	De security wordt afgezwakt of zelfs ~~opengezet~~ niet uitgevoerd	X	X		X		5	3	15	Security configuratie en installatie richtlijnen opstellen Valideren van juiste security instellingen (tooling?: bijv. checken gewenst gedrag bij niet geauthoriseerde toegang, …)	Security controle uitvoeren op straat: hoe? Automatisch, periodiek? --> audit-plan maken.	Security gegevens non-recoverable verwijderen		5	1	5
			Authentificatie mislukt, er kan geen verbinding gemaakt worden			X			2	3	6	Security configuratie en installatie richtlijnen opstellen	Security controle uitvoeren op straat	Security gegevens verwijderen		5	1	5

Subject	Threats	Effect	Confidentiality	Integrity	Availability	Authenticity	Reliability	Impact	Probability	Risk	Measures				Impact	Probability	Risk
	Geclassificeerde informatie wordt gemodificeerd of gekopieerd op het moment dat de apparatuur toegankelijk is wat is toegankelijk? Een VRI langs de kant van de weg; is die altijd toegankelijk?	De security-maatregelen kunnen door onbetrouwbare of onbevoegde personen of Applicaties worden gepasseerd op een later moment.	X	X	X	X		5	2	10	Apparatuur met (toegankelijke) geclassificeerde informatie alleen toegankelijk voor geauthoriseerd personeel	Security controle regelmatig laten uit voeren en onderhouden: Hoe? Security settings regelmatig veranderen Security settings dusdanig opslaan dat deze niet toegankelijk zijn voor onbevoegden	Security gegevens non-recoverable verwijderen		2	1	2
	Er wordt software of hardware aan de apparatuur toegevoegd om security settings te stelen (theft)	De security settings kunnen door onbetrouwbare of onbevoegde personen worden achterhaald voor misbruik op een later moment	X	X	X	X		5	2	10	Apparatuur met (toegankelijke) geclassificeerde informatie alleen toegankelijk voor geauthoriseerd personeel	Controle en onderhoud uitvoeren Security settings regelmatig veranderen Security settings dusdanig opslaan dat deze niet toegankelijk zijn voor onbevoegden	Security gegevens non-recoverable verwijderen		2	1	2
	Na deinstallatie / afvoer wordt geclassificeerde informatie of componenten niet verwijderd of gewist	De security settings kunnen door onbetrouwbare of onbevoegde personen worden achterhaald voor misbruik op een later moment	X	X	X	X		3	2	6	Deinstallatie richtlijnen opstellen	Security settngs regelmatig veranderen	Security gegevens non-recoverable verwijderen		1	1	1
Centrale apparatuur	Centrale apparatuur/software wordt niet correct geinstalleerd	ITS Applicaties lopen niet goed waardoor het gedrag van de iTLC leidt tot instabiele of verkeersonveilige situaties			X			5	2	10	Controle, test, installatie en deinstallatie richtlijnen opstellen	Monitoring van ITS Applications op de centrale apparatuur	Deinstalleren overeenkomst de gestelde richtlijnen		5	1	5
	Geclassificeerde informatie wordt gemodificeerd of gekopieerd op het moment dat de apparatuur toegankelijk is (bijv. in magazijn of tijdens vervoer)	De security settings kunnen door onbetrouwbare of onbevoegde personen worden achterhaald voor misbruik op een later moment	X	X	X	X	X	5	2	10	Apparatuur met (toegankelijke) geclassificeerde installatie niet toegankelijk voor onbevoegden Toevoegen van security settings pas na installatie (bijv. in SAT-fase), wanneer de apparatuur beschermd is tegen fysieke, onbevoegde toegang Secure opslaan van security settings	Security controle regelmatig laten uit voeren en onderhouden Security settings regelmatig veranderen	Security gegevens verwijderen		2	1	2
	Er wordt software of hardware aan de apparatuur toegevoegd om security settings te stelen (theft)	De security settings kunnen door onbetrouwbare of onbevoegde personen worden achterhaald voor misbruik op een later moment	X	X	X	X	X	5	2	10	Apparatuur met (toegankelijke) geclassificeerde informatie alleen toegankelijk voor geauthoriseerd personeel Secure opslaan van security settings	Controle en onderhoud uitvoeren Security settngs regelmatig veranderen	Security gegevens verwijderen		2	1	2
	Na deinstallatie / afvoer wordt geclassificeerde informatie of componenten niet verwijderd of gewist	De security settings kunnen door onbetrouwbare of onbevoegde personen worden achterhaald voor misbruik op een later moment	X	X	X	X	X	5	2	10	Deinstallatie richtlijnen opstellen	Security settngs regelmatig veranderen	Security gegevens verwijderen		1	1	1
Behuizingen / kast	Kast wordt niet goed geinstalleerd	zie Wegkantapparatuur															
	Kast is toegankelijk voor onbevoegden tijdens installatie	De security settings kunnen door onbetrouwbare of onbevoegde personen worden achterhaald voor misbruik op een later moment	X	X	X	X	X	5	2	10	Security settings pas na installatie toevoegen in de iTLC	Kast moet afsluitbaar zijn	Security gegevens verwijderen		5	1	5
	Er wordt hardware of software toegevoegd om security settings te stelen (theft)	De security settings kunnen door onbetrouwbare of onbevoegde personen worden achterhaald voor misbruik op een later moment	X	X	X	X	X	5	2	10	Apparatuur en software controleren op afwijkingen Secure opslag van Security settings	Kast moet afsluitbaar zijn	Security gegevens verwijderen		5	1	5
	Kast is toegankelijk (bijv. in magazijn of tijdens vervoer)	De security settings kunnen door onbetrouwbare of onbevoegde personen worden achterhaald voor misbruik op een later moment	X	X	X	X	X	5	2	10	Security settings pas na installatie toevoegen in de iTLC	Kast moet afsluitbaar zijn	Security gegevens verwijderen		5	1	5
Service tooling (laptops)	Software worden niet goed geinstalleerd	De iTLC wordt met corrupte software of configuratie geladen en kan daardoor niet correct functioneren			X			1	2	2	Richtlijnen voor installatie van service tooling	Controle en onderhoud van service tooling	Service tooling na inleveren compleet wissen		1	1	1
	Tools bevatten classificatie gegevens en zijn toegankelijk	De security settings kunnen door onbetrouwbare of onbevoegde personen worden achterhaald voor misbruik op een later moment	X	X	X	X	X	5	2	10	Service tooling voorzien van autorisatie mechanisme	Autorisatie gegevens op regelmatige basis wijzigen	Service tooling na inleveren compleet wissen		5	1	5
	Er wordt afluistersoftware geinstalleerd	De security settings kunnen door onbetrouwbare of onbevoegde personen worden achterhaald voor misbruik op een later moment	X	X	X	X	X	5	2	10	Service tooling voorzien van autorisatie mechanisme	Controle en onderhoud van service tooling	Service tooling na inleveren compleet wissen		5	1	5

Subject	Threats	Effect	Confidentiality	Integrity	Availability	Authenticity	Reliability	Impact	Probability	Risk	Measures				Impact	Probability	Risk
	Servicetooling wordt gekopieerd/geinstalleerd door onbevoegden	Onbevoegde personen kunnen tooling installeren op eigen hardware en hiermee configuratie van een iTLC wijzigen	X	X		X	X	5	2	10	Installatie van software voorzien van authorisatie mechanisme zodat deze alleen door bevoegden personen te installeren is.	Service tooling beveiligen tegen gebruik door onbevoegden			5	1	5
Productie tooling	Productie tooling is niet correct geinstalleerd	De iTLC kan worden verzien van foutieve software of configuratie en kan daardoor niet correct functioneren			X			1	2	2	Richtlijnen voor productie en productie apparatuur instellen Geen security informatie aan de producent beschikbaar stellen				1	1	1
	Productie tooling bevat geclassificeerde gegevens en zijn onbeheerd	De security settings kunnen door onbetrouwbare of onbevoegde personen worden achterhaald voor misbruik op een later moment			X			2	2	4	Richtlijnen voor productie en productie apparatuur instellen Geen security informatie aan de producent beschikbaar stellen				2	1	2
	Er wordt afluistersoftware geinstalleerd	De security settings kunnen door onbetrouwbare of onbevoegde personen worden achterhaald voor misbruik op een later moment			X			2	2	4	Richtlijnen voor productie en productie apparatuur instellen Geen security informatie aan de producent beschikbaar stellen				2	1	2
	Productietooling wordt gekopieerd/geinstalleerd door onbevoegden	Onbevoegde personen kunnen tooling installeren op eigen hardware en hiermee configuratie van een iTLC wijzigen	X		X	X		2	2	4	Installatie van software voorzien van authorisatie mechanisme zodat deze alleen door bevoegden personen te installeren is.	Service tooling beveiligen tegen gebruik door onbevoegden			2	1	2
Access control																	
User access management	Ongeauthoriseerde toegang	De regeltoestand wordt negatief beinvloed De verkeersveiligheid wordt negatief beinvloed De verkeerde LDM objecten worden aangemaakt De functies van TLC-FI en RIS-FI worden misbruikt De IVERA interface kan worden misbruikt of foutief gebruikt		X	X			5	2	10	Autorisatie en Authenticatie mechanisme inbouwen	Autorisatie en Authenticatie beheren	Autorisatie en Authenticatie gegevens verwijderen		3	1	3
	Vekeerde rol / of toegangsrechten	De regeltoestand wordt negatief beinvloed De verkeersveiligheid wordt negatief beinvloed De verkeerde LDM objecten worden aangemaakt De functies van TLC-FI en RIS-FI worden misbruikt of kunnen niet worden gebruikt De IVERA interface kan worden misbruikt of foutief gebruikt		X	X			5	2	10	Rol en toegangsrechten beheerplan opstellen	Rol en toegangsrechten beheerplan uitvoeren Logging van wijzigingen	Rollen en toegangsrechten verwijderen		3	1	3
	Geen toegang (bijv. tot politie-paneel)	De regeltoestand kan niet worden beinvloed De verkeersveiligheid kan niet worden verbeterd			X			3	2	6	Sleutelbeheer plan	Toepassen goed sleutel beheer	Sleutel inname procedure volgen		1	1	1
User responsibilities (*make users accountable for safeguarding their authentication information*)	Onverantwoordelijk gedrag van mensen zorgt ervoor dat authenticatie gegevens verspreid raken. Gevolgen ook bijv. auditing, traceability, etc Kan ook zijn dat mensen vergeten uit te loggen waardoor onbevoegden toegang hebben	regeltoestand wordt negatief beinvloed verkeersveiligheid wordt negatief beinvloed verkeerde LDM objecten worden aangemaakt functies van TLC-FI en RIS-FI worden misbruikt		X		X	X	5	5	25	Authenticatie policy opstellen en deze in de iTLC implementeren. Bijvoorbeeld: * registratie en bewaking van niet-succesvolle en succesvolle inlogpogingen * inactieve sessie beeindigen	Authenticatie policy volgen	Authenticatie gegevens verwijderen		5	2	10
System en applications access control (M2M)	Ongeauthoriseerde access	De regeltoestand wordt negatief beinvloed De verkeersveiligheid wordt negatief beinvloed De verkeerde LDM objecten worden aangemaakt De functies van TLC-FI en RIS-FI worden misbruikt De IVERA interface kan worden misbruikt of foutief gebruikt		X	X			5	2	10	Autorisatie en authenticatie mechanisme inbouwen voor ITS applications	Autorisatie en Authenticatie beheren	Autorisatie en Authenticatie gegevens verwijderen		5	1	5
	Verkeerde (of geen) rol / permissions	De regeltoestand wordt negatief beinvloed De verkeersveiligheid wordt negatief beinvloed De verkeerde LDM objecten worden aangemaakt De functies van TLC-FI en RIS-FI worden misbruikt De IVERA interface kan worden misbruikt of foutief gebruikt		X	X			5	3	15	Rol en toegangsrechten beheerplan opstellen voor ITS applications	Rol en toegangsrechten beheerplan uitvoeren	Rollen en toegangsrechten verwijderen		5	1	5
	Geen toegang (bijv. regelen niet mogelijk)	Regeltoestand kan niet worden beinvloed verkeersveiligheid kan niet worden verbeterd			X			5	3	15	Rol en toegangsrechten beheerplan opstellen voor ITS applications	Rol en toegangsrechten beheerplan uitvoeren	Rollen en toegangsrechten verwijderen		5	1	5

	Subject	Threats	Effect	Confidentiality	Integrity	Availability	Authenticity	Reliability	Impact	Probability	Risk	Measures				Impact	Probability	Risk
Cryptography																		
	Ensure proper and effective use of cryptography	Verouderde cryptography toegepast	Security mechanismes worden afgezwakt	X	X		X		4	3	12	Plan opstellen voor het toepassen van cryptography	Beheerplan uitvoeren	Verwijderen cryptography gegevens		4	1	4
		Gebruikte cryptography methode veroudert en wordt niet geupdate	Security mechanismes worden afgezwakt	X	X		X		4	5	20	Plan opstellen voor het toepassen van cryptography	Beheerplan uitvoeren	Verwijderen cryptography gegevens		4	1	4
		Incorrect key-management (public/private key): storage, distribution, lifetime	Security mechanismes worden afgezwakt	X	X		X		4	3	12	Plan opstellen voor het toepassen van cryptography	Beheerplan uitvoeren	Verwijderen cryptography gegevens		4	1	4
Physical and Environmental security																		
	Fysieke toegang	ongeoorloofde fysieke toegang tot compartimenten van de kast	Regeltoestand wordt negatief beinvloed Verkeersveiligheid wordt negatief beinvloed			X			5	2	10	Behuizing voorzien van sloten	Sleutelbeheerplan uitvoeren	Sleutel inname		5	1	5
		ongeoorloofde fysieke toegang tot netwerkapparatuur in de kast	Security mechanismes worden afgezwakt of gekraakt	X	X	X	X	X	5	2	10	Behuizing voorzien van sloten	Sleutelbeheerplan uitvoeren	Sleutel inname		5	1	5
		ongeoorloofde fysieke toegang tot netwerkbekabeling buiten de kast	Regeltoestand wordt negatief beinvloed Verkeersveiligheid wordt negatief beinvloed Security mechanismes worden afgezwakt of gekraakt	X	X	X	X	X	5	3	15	Firewall toepassen en encryption Netwerkbekabeling fysiek afschermen				5	1	5
		ongeoorloofde toegang tot server ruimte	Regeltoestand wordt negatief beinvloed Verkeersveiligheid wordt negatief beinvloed Security mechanismes worden afgezwakt of gekraakt	X	X	X	X	X	5	2	10	Toegangsmechanisme voor de serverruimte	Toegangsbeheer uitvoeren			5	1	5
Operations Security																		
	Operational procedures and responsibilites (To ensure correct and secure operations of information processing facilities)											*Prior to installation*	*During operation*	*After deinstallation*				
		Unclear operational procedures	No clear operational and change procedures causes weaker security mechanisms that rely on proper operations		X	X	X		3	3	9	*Define operational procedures (installation, configuration, service, maintnenace and change procedures)*				3	1	3
	- replacement of hardware components	Credentials are not unrecoverably removed from replaced hardware.	Credentials can be determined by unreliable or unauthorized persons for abuse		X		X		5	2	10	Define repair proces	Lifetime on security data. Use repair proces.	Follow procedures for deinstallation		1	1	1
	- software update	Updated software does not meet security requirements. (e.g. aged software or due to new features)	Degraded security measures		X		X		2	2	4	Define update proces Define software validation proces. Automate update proces				2	1	2
		Configuration is not updated and contains default accounts.	Degraded security measures default accounts can be used for unauthorised access.		X		X		2	2	4	Use safe defaults Check configuration version.				2	2	4
		Development, test and production systems are mixed resulting in development or test access in production systems.	Unauthorized access to production systems		X		X		2	2	4	Use seperate develop, test and production environments				2	2	4
	'- (hand)bediening	Leave location without closing and or logging out.	Unauthorized person can gain access with an open session.		X	X	X		2	2	4	Define operational procedures	Use timeout after idle time. Logging off after closing cabinet.			2	2	4
	Protection from malware	Unauthorized software (Malware) can be installed.	Credentials can be copied. Communication can be tapped. Installation of other malware. Local network can be connected to external server.		X	X	X		4	2	8	Analyse risks for used components. Use firewalls and virus scanners if applicable.	Update virus definitions. Monitor and react on reported infections.			4	2	8
		Release server with new releases may contain unautorized software which then is considered part of a distributrion	During update of an iTLC, unwanted software is installed as part of the released package.		X	X	X		4	1	4	Define update proces. This proces should contain measures for unauthorized access.	Use latest update proces.			4	1	4
		Unauthorized software is installed on tools used for the iTLC (service tools etc.)	Tools are compromised. May be source of weakness.		X		X		4	2	8	Implement policy to use only authorized software	Autorization procedure for software Use tools to detect malware			4	2	8
	Backup																	

Subject	Threats	Effect	Confidentiality	Integrity	Availability	Authenticity	Reliability	Impact	Probability	Risk	Measures				Impact	Probability	Risk
- Stored backup data.	Theft of security data/credentials from back-up storage.	Unauthorized access with stolen credentials		X		X		4	1	4	Restricted acces to backup (authentification, encryption)				4	1	4
	Unauthorized access to security data.	Security measures can be weakened or hacked.		X		X		4	1	4	Policy for back-up of credentials				4	1	4
	Unauthorized access to privacy data.	Privacy data can be abused.	X					3	1	3	apply at least the same storage access rights for back-up data as the operational dala.				3	1	3
- Security data that is not backed up.	No recovery of system (parts).	System not available / long recovery duration.			X			3	3	9	Define procedure for back-up of security data. Define procedure for requesting new credentials.				3	3	9
Logging and Monitoring (security-scope). To record events and generate evidence.																	
loggig of events	Insufficient or no logging of exceptions, security events.	No detection of security incidents. (e.g. failed access attempts) No traceability possible of performed actions. (who, when, action)		X		X		2	2	4	Define procedure for auditing the eventlog. Implement eventlog. (Activities applications and users as exceptions, faults and security events.) Add e.g. door contacts to monitor/log fysical access.	Check eventlog using the auditing procedure			2	2	4
	Insufficient or no logging of performed updates or other events.	No traceability possible of performed updates and their result.		X	X	X		2	2	4	Implement logging				2	2	4
access	Logging is accesible by unauthorized persons. Log contains (parts of) credentials.	Credentials can be obtained from log.		X		X		3	1	3	Only allow access to logs within a secured channel. Only allow access to security log for authorised users Don't log credentials sufficient to gain access				3	1	3
	log not protected against unauthorized modifications (including removing)	security-issues cannot be detected or analyzed (e.g. unsuccessfully access attempts).		X		X		4	1	4	Log events (also) on remote system. Protect log from being altered Implement mechanisms to detect tampering of logs				4	1	4
door contact	Opening and closing door is not detected/logged.	Unauthorized physical access to iTLC possible without logging and ability to check.		X		X		2	2	4	Implement door contact and log this				2	2	4
Time synchronisation	Event logs from different systems cannot be synchronized with each other.	Analyzing for auditing is difficult or not possible			X			2	2	4	Use time synchronization on all systems. Make sure that time changes are logged in the eventlog so that actual time can always be identified.				2	2	4
Control of operational software (To ensure the integrity of operational systems)																	
ensure integrity of operational software and configuration	configuration has been changed by unauthorized persons/applications	after installation, security measures degraded		X		X		3	1	3	need a way to detect changes in configuration/security settings	Ensure integriteit of operational software and configuration			3	1	3
	Aged software has less/non secured access points.	Security is bypassed over aged protocols.				X		3	2	6	Block unsecured protocols.				3	2	6
	update not working	Applied update not effective.			X			2	2	4	Define Contingency plan. Software parts should provide version information.	Verify versions of software.			2	2	4
	rollback not working	System (partly) not available			X			3	2	6	Define recovery procedure.	Manual installation of software if rollback fails.			3	2	6
	release packcage of software has been altered	malicious software could be installed as part of the release		X		X		4	2	8	check integrity of release package by validating software with a central repository?				4	2	8
	Operational software has aged protection	Security is not sufficient any more.		X		X		2	3	6	Define plan for scurity upgrades.				2	3	6
Technical vulnerability management (To prevent exploitation of technical vulnerabilities)																	

	Subject	Threats	Effect	Confidentiality	Integrity	Availability	Authenticity	Reliability	Impact	Probability	Risk	Measures				Impact	Probability	Risk
	monitor technical vulnerabilities of used system/components. (including routers, firewals, software libaries.)	(new) exploits are not analysed (risk, impact)	High risk exploits do not trigger the update with new release packages (patch) and the deployment of it. The iTLC stays vulnerable for this exploit.		X		X		3	2	6	Setup process with suppliers to monitor found weaknesses and patches for software and hardware components. Define response time for technical vulnerabilities based vulnerability risk assessment (See also: asset control)	Define alternative mitigation actions for each exploit. (e.g. switching off some services.)			3	2	6
		No updates performed to mitigate weaknesses/exploits	iTLC will be more vulnerable in time.		X		X		2	3	6	Setup process with suppliers iTLC. Automate frequently update of software and support/allow this.	Monitor technical vulnerabilities of used system/components ook bijv. router, firewall, used sw-libs			2	3	6
		New software release contains exploit.	Exploit will be (re-)introduced on iTLC.		X		X		3	2	6	Create acceptance rules for new software releases.				3	2	6
	Information systems audit considerations (To minimise the impact of audit activities on operational systems)	No security auditing is performed.	Unknown system security state.		X		X		2	3	6	Add auditing functions to iTLC. Define minimal requirements for this and include this in design and test.	Audit security of iTLC (Current accounts, versions, are procedures correctly implemented and used.)			2	3	6
		Auditing interfers with operational tasks of iTLC.	Primary tasks of iTLC are affected. Bad or no performance of iTLC during auditing.			X			2	1	2	Add auditing functions to iTLC. Define minimal requirements for this and include this in design and test.	Audit during times of minimal impact on availability,			2	1	2
	Privacy road user	Road user movements can be tracked by gathering messages from Vehicle.	Organization can obtain behavior of individuals.	X					4	3	12	Using pseudo ID's and pseudo certificates to split up traces.				3	2	6
Communications security																		
	Network security management (To ensure the protection of information in networks and its supporting processing facilities																	
	Logically and physically separated	Internal network not separated from external network. (e.g. PTP communication using IP.)	Unauthorized systems on the external network can access internal systems (e.g. RIS-FI or TLC-FI).		X		X		3	2	6	Separate network logical and or physical.				3	1	3
		Internal network not sepparated from networkconnection with G5-modem	Unauthorized systems on the external network can access internal systems (e.g. RIS-FI or TLC-FI).		X		X		3	3	9	Separate network logical and or physical.				3	1	3
		ITS-Application creates own VPN connection. (With external system)	internal network not separated from external networks		X		X		5	1	5	Use firewall with strict rules. Also for internal traffic. (e.g. when third party adds host to iTLC with ITS-application.).				2	1	2
	Information transfer (To maintain the security of information transferred within an organization and with any external entity)																	
	maintain of security information transferred	Credentials can be copied. (e.g.Maintenance activities, replacement TLC)	Unauthorized access to iTLC		X		X		4	2	8	procedure cryptography automating?				4	1	4
		ITS G5 messages not signed	receiver cannot determine is sender is to be trusted		X				3	5	15	setup PKI so that messages can be signed and validated (according to ETSI standards)				3	2	6

	Subject	Threats	Effect	Confidentiality	Integrity	Availability	Authenticity	Reliability	Impact	Probability	Risk	Measures				Impact	Probability	Risk
	Sniffing	Sniffing on physical external parts of the internal network. The gathered data can be monitored and stored.	Exchanged data is available for unauthorized persons. (credentails, commands).				X		3	1	3	Data encryption. (Networkhost, interface or session??)				3	1	3
	Denial of service	DDOS	iTLC-interfaces not available for ITS-Applicaties			X			3	3	9	Use firewall with DDOS protection Have internal back-up application available				2	2	4
		Brute force attack may disable user-account	Authorized ITS-Application may not be able to login			X			3	2	6	Define actions to take faced with a brute-force attack without having to disable the user-account (E.g. Reject access from an IP, only allow a number of subsequent failed accesses from a host, implement timeouts disabling access for alimited time which makes brute foce attacks less efficient)				3	1	3
System acquisition, development and maintenance																		
	security of purchased items	components contains unacceptable security risks	degraded security of iTLC		X	X	X	X	4	2	8	* test items before deployment * update firmware (0-day exploits) * whitelist of accepted items * For each item: record accepted versions/revisions and create agreements with suppliers to supply only this versions/revisions				4	1	4
	security in development and support process	implementation of measures introduces new vulnerabilities/risks	degraded security of iTLC		X	X	X	X	3	3	9	coding guidelines security requirements in design knowledge capabilities developers	Ensure information security is implemented and designed within development lifecycle with knowledge and process to ensure no vulnerabilities are introduced			3	2	6
	-- ensure information security is implemented and designed within development lifecycle with knowledge and process to ensure no vulnerabilities are introduced	Development environment not protected	Environment accessible for unauthorized persons.		X	X	X		3	2	6	secure access to development environment				3	1	3
	update operating system	if operating system is not updated, the iTLC could become more vulnerable to exploits.	degraded security of iTLC				X		3	3	9	Setup process with suppliers to monitor patches for software and hardware components.	Deploy patches to system.			3	2	6
	life cycle support, versioning, etc	use of EOL-products/components	using old standards or products can degrade security measures (e.g. old encryption standard)				X		3	2	6					3	2	6
		frequent software releases with increasing number of features	degraded security of iTLC due new features or less test effort				X		3	2	6					3	2	6
	Testing of systemsecurity	security measures are not tested during development	degraded security of iTLC		X	X	X		3	3	9	* use automated test (like tools to analyse codes or scan for vulnerabilities * Verify repairs of security realated issues.				3	1	3
		test data accesible for unauthorized persons.	Credentials can be determined by unreliable or unauthorized persons for abuse		X	X	X		4	2	8	Use seperate develop, test and production environments				4	1	4
	Product sources	Analysing sources can be used to gain unautorized access.	degraded security of iTLC		X		X		4	2	8	store sources secure (e.g. source code)				4	1	4
Supplier relationships																		
	outsourcing:	3rd party may break security measures	degraded security of iTLC		X		X		4	2	8	Qualification and selection				4	1	4

	Subject	Threats	Effect	Confidentiality	Integrity	Availability	Authenticity	Reliability	Impact	Probability	Risk	Measures				Impact	Probability	Risk
	- datacentre (e.g hosting Applications)																	
	- network supplier/provider																	
	- maintenance can be outsourced																	
Information security incident management																		
	Management of information security services	No incident management proces defined	security incidents not reported/registered.	X	X	X	X	X	3	3	9	Define incident management proces (with reponcibilities)	Review after every incident the proces to maintain and improve it.			3	2	6
		incident management proces not excecuted	No effective follow up after a security security incident	X	X	X	X	X	3	2	6	Review proces with proces users before proces excecution.	Regulary proces evaluation and maintain and improve it.			3	1	3
		security incident related to architecture/interface-definition not shared with other iTLC suppliers	incident may be repeated on iTLC of other manufacturers without knowing	X	X	X	X	X	3	2	6	Define incident management also on iTLC-level				3	1	3
		security incident not reported/registered/handled :	incident may be repeated without knowing	X	X	X	X	X	3	2	6	Educate Employe Automate reporting?				3	1	3
		reported incident accessible by unauthorized person	can be used to exploit deployed vulnerable systems before they are patched	X	X	X	X	X	3	2	6	define strict access to database of reported incidents. Use authentication before accessing database (How to deal with security incidents regarding this database?)				3	1	3
		security measures not updated due to reported incidents	deployed iTLC's stay vulnerable				X		2	4	8					2	4	8
		security incident not reported/registered/handled.	incident may be repeated without knowing				X		1	3	3					1	3	3
		reported incident accessible by unauthorized person	abuse of information e.g. for another attack				X		2	2	4					2	2	4
		security measures not updated due to reported incidents	incident may be repeated	X	X	X	X	X	3	2	6					3	2	6
information security aspects of business continuity management																		
	The Organization should register its demands for information security and for the continuity of the information security management in adverse situations, eg. a crisis or disaster.	business continuity can be at risk when safety critical information/vulnerable becomes public or systems are no longer accessible.				X			3	2	6	Maintaining and using this matrix				2	1	2
Compliance																		
	Prevention of violations of legal, statutory, regulatory or contractual obligations concerning information security and security requirements.																	
	Legal standards	no compliance with regulations (national/international)						X	4	2	8					4	2	8
	Regulatory	no compliance with updated regulations (national/international)						X	4	2	8					4	2	8

iVRI Safety matrix

Subject	Threat	Effect	Initial Impact	Initial Probability	Initial Risk	Measure				Remaining Impact	Remaining Probability	Remaining Risk
Availability of in Car information as transmitted by iTLC												
						Prior to operation	*During operation*	*Post operation*				
Traffic application	No traffic signal prediction information available	Road user has no in Car information about traffic signal predictions	1	5	5	Quality test of application regarding timing predictions.	Quality monitoring during operation			1	3	3
	Traffic application reboots	Road user has no in Car information about traffic signal predictions	1	2	2					1	2	2
TLC	Actual traffic signal information not updated	Road user has old in Car information	3	3	9		Use appropriate life time of data			3	1	3
	TLC-FI is rebooting or temporarely not available	Road user has no in Car information about traffic signal predictions	1	2	2	Certification of iTLC systems	Use appropriate life time of data			1	1	1
RIS	RIS is rebooting or temporarely not available	Road user has no in Car information about traffic signal predictions	1	2	2	Certification of iTLC systems	Use appropriate life time of data			1	1	1
	Congestion at radio-level	ITS G5 messages transmitted with delay or not all.	4	1	4		handle in implemented use-case			2	1	2
	RIS is rebooting or temporarely not available	ITS G5 messages cannot be received or transmitted by iTLC.	4	1	4		handle in implemented use-case			2	1	2
OBU	Receiving ITS-station can not determine if the sender of ITS messages can be trusted.	In car information is no longer available	1	3	3	Sign transmitted messages and validate received messages according to ETSI standards.	Do not display information that is based on expired data			1	1	1
	Send MAP ITS-messages are not received by ITS-station (VIS)	Received SPaT data is not useable	1	2	2		Do not display information if MAP data is not present or up to date Send MAP messages on a regular bases			1	1	1
	Send SPat ITS-messages are not received by ITS-station (VIS)	In car information is no longer available or conflicting with actual traffic light signals.	3	5	15	Use appropriate life time of data	Use appropriate life time of data Periodic transmissions of SPaT messages			3	1	3
Correctness of in Car information												
						Prior to operation	*during operation*	*Post operation*				
Timing	Time synchronisation difference too large between TLC and Vehicle.	In car information conflicts with traffic light signals.	5	3	15	All systems in the iTLC environment must be time synchronised. If components are not synchronized they must not send or present information. iTLC must be certified regarding timesynchronization and delays	Predictions are absolute time from TLC.			3	1	3
	Time delay between actual signal state change and in car information is too long.	In car information conflicts with traffic light signals.	5	5	25		transmit actual state changes at radio level within 500 msec.			3	3	9
Authorisation	Unauthorisized application may publish SPaT or MAP information.	In car information conflicts with traffic light signals.	5	2	10	See Security matrix	See Security matrix	See Security matrix		5	1	5
Signalgroup timing	Signal group timing and prediction estimates are not correct	In car information conflicts with traffic light signals estimates.	5	3	15	Quality test of application regarding timing predictions.	TLC checks the signal group state and timing at run time			3	1	3
	Signal group estimates changing inconsequently - (Priority) request	The in car information can not reliably be determined.	5	5	25		TLC also checks the signal group estimates changes, and takes appropriate measures			3	1	3
	Signal group actual state does not corresponding with SPaT information.	In car information conflicts with traffic light signals.	5	3	15	Certification of iTLC systems	TLC checks the signal group state and timing at run time			5	1	5
SPaT/Map	Map data conflicts with intersection topologie.	In car information conflicts with traffic light signals.	5	1	5	Define process to provide the appropriate Map data to the iTLC				5	1	5
	Spat data conflicts with Map data.	In car information conflicts with traffic light signals.	5	1	5	Define process to check Map and Spat data in advance	Check SPaT data against the MaP data continuesly, and stop sending Spat data if necessary			5	1	5

	Subject	Threat	Effect	Impact	Probability	Risk	Measure				Impact	Probability	Risk
	TLC error	If major fault causes TLC to amber blinking immediatly then signal group information is not updated fast enough.	In car information conflicts with traffic light signals.	1	3	3	Certification of iTLC systems	Update traffic state immediate and set signal group information to unknown or amber flashing. Transmit state as SPAT-message within 500 msec			1	1	1
	iTLC	Incorrect processing of data	Incorrect advise/information	5	3	15		Acceptance procedure for OBU applications			5	1	5
		Incorrect position	Incorrect advise/information	5	3	15		Check position against history and map data.			5	1	5
Road user													
	OBU	Wrong Interpretation presented information	Unsafe driving behaviour like red light negation or not start driving on green light.	5	3	15	Present information to support driving functions but force user to have final view on traffic lights.				5	1	5
	OBU	Unintended use of information. (Like driving at maximum speed over the stop line at start green using time to green value)	Calculation of clearing times does not cover this behaviour resulting in unsafe situations.	5	3	15	Presenting information only for intended use. (E.g., not presenting time to green if driving but a speed advice indication with as target a normal stop distance from stop line at start green.)	Specify intended use of data.	Specify restrictions for data use.		5	1	5
	OBU	Driver is distracted by the use of the OBU.	No attention to other traffic, traffic lights or signs	3	3	9	OBU must be in sight or integrated in vehicle console	Use also sound or other senses for directions			3	2	6