Your Security Partner

Si-TaRA

Si-Tara

Threat analysis and Risk Assessment

Sai Kumar Reddy

2023-11-14T07:23:37.328Z

Threat and Risk Analysis & Residual Risk Analysis

1) Metadata

Please enter Metadata.

Project Name	Si-Tara
Project Number	-
Document Name	
Document Version	
Template Version	V 2.3.2, 04.12.2019
Document Responsible	
Document Status	Please select
Confidentiality	Please select
Methodology	Attack Potential

If this TRA is an adaptation of a reference project TRA:

Reference Project Name	
Reference Project Number	
Link to Reference Project TRA	

2) Change History

Please document changes.

Revision	Remarks	Author

3) Document Information

• In each sheet the lighter colors indicate the cells that need to be filled in. The cells with darker colors will be filled in automatically.

• In the sheets Assumptions, MUCs, DSsConsequences, SecGoals, ThreatsDSs, ThreatEvaluation_AP/LE, RiskAssessment_AP/LE and SecurityNeeds_AP/LP you find yellow tables with examples for filling out the template.

Sheet Name	Description	How to use
About	The sheet contains a short description of this workbook, information about the usage, meta data and a change history.	Please enter the metadata and document changes. Please note that the template needs to be classified as "Confidential" once it is filled out (even partially). Please select a methodology.
Methodology	This sheet contains an overview of the supported Threat and Risk Analysis (TRA) methodologies and a list of specific terms and definitions.	This sheet is informative.
TechDescription	The sheet is intended to contain a technical description of the target of evaluation (TOE) which enables the reader to retrace the TRA.	Please give a technical description of the TOE. Please include graphics describing the physical and logical architecture. Alternatively you may refer to a separate document describing the TOE. Here it must be ensured that the reference remains available as long as the TRA is valid.
Scope	The sheet is intended to state the scope of this analysis.	Please describe the scope of this TRA.
Assumptions	The sheet is intended to state the assumption which are made for this analysis.	Please list the assumptions made for this TRA.
MUCs	This sheet is intended for the documentation of identified misuse cases. The sheet is optional, depending on whether you are working with misuse cases or not.	If you are working with misuse cases, please list them in this sheet. Otherwise, skip the sheet.
DSsConsequences	This sheet is intended to contain all relevant damage scenarios together with their consequences. It provides the consequence classification table from Bosch Norm N103 SEC002.	Please enter all relevant damage scenarios and assign the suitable consequences according to the consequence classification table. Please document where the damage scenario comes from by 1. citing one or more misuse cases or 2. giving another reason. Please give also a reason why you choose the specific consequence.
SecGoals	This sheet is intended to give a list of all relevant security goals.	Please list all relevant assets and choose the related security objectives. Please describe each security goal (asset, objective) and give a reason for the relevance.
ThreatsDSs	This sheet contains the definition of the threats and the n:m-relation between the threats and the damage scenarios.	Please give a description of each threat and select all damage scenarios it leads to. Give a reason why the threat can result in the specific damage scenario.
ThreatEvaluation_AP	This sheet is intended to contain the attack potentials of the threats. Additionally, possible scaling effects are to be documented here. This sheet refers to method a) described below. It provides a slight modification of the Common Criteria Attack Potential Scale which should be used for this analysis.	For each threat create an attack tree file (for example with MS-Visio). Please add a link to the file or include the graphic in the sheet AttackTrees. Please document the attack potential and describe possible scaling effects of the threats.
ThreatEvaluation_LE	In this sheet the likelihoods of the threats are to be estimated. Additionally, possible scaling effects are to be documented here. This sheet refers to method b) described below. It provides the Threat Likelihood Assessment Table from Bosch Norm N103 SEC002 which should be used for this analysis.	Please estimate the likelihoods of the threats according to the threat likelihood assessment table and give reasons for your choice. Please describe possible scaling effects of the threats.
AttackTrees	This sheet provides space for the attack trees.	Alternatively to providing links to external attack tree files in sheet ThreatEvalutaion_AP you can insert pictures/graphics of the attack trees and additional information about the attack trees here.
RiskAssessment_AP	This sheet performs the risk assessment automatically. For each damage scenario the risk is calculated from its consequence and from the minimum attack potential of all threats that lead to it. The sheet refers to method a)	Will be generated automatically.
RiskAssessment_LE	This sheet performs the risk assessment automatically. For each damage scenario the risk value is calculated from its consequence value and from the maximum likelihoods of all threats that lead to it. The sheet refers to method b)	Will be generated automatically.
SecurityNeeds_AP/LE	This sheet contains the security needs which arise from the security risks, from the assumptions and from Bosch or customer requirements. The responsible for the specific security needs is named here.	Please formulate the security needs from the risks, assumptions and RB/customer requirements. Give reasons for the needs and identify the responsible.
MngSummary_AP/LE	The sheet is intended to give a management summary in text form. It also provides an overview table containing the damage scenarios, the related risks and possible scaling effects.	Please write a management summary and summarize possible scaling effects of the threats leading to the related damage scenario.

4) Template Version History

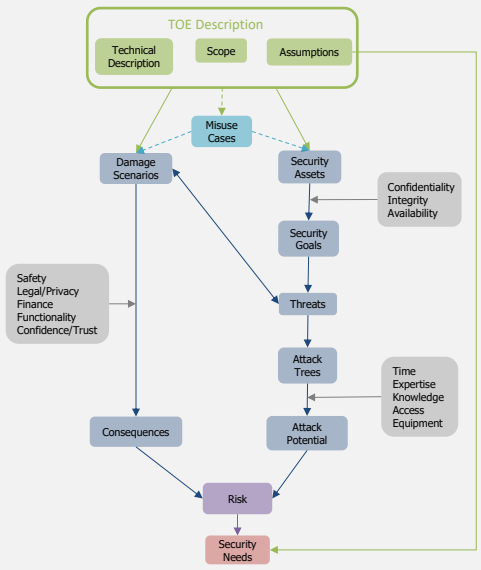
Version number/date	Changes regarding previous version
1.0	Creation of template
2.0	tbd
2.1	tbd
2.1.1	tbd
2.1.2	tbd
2.1.3	tbd
2.1.4	tbd
2.2	tbd
2.2.1/17.05.2018	* *SecurityNeeds_AP/LE*: Numeration of security needs improved
2.3/26.10.2018	* *About*: Button for method selection added * *About:* Template History added * *Methodology*: Attack potential table added * *SecGoals*: Security goals "authenticity", "freshness", "correctness", "access control" added * *Assumptions, MUCs, DSsConsequences, ThreatsDSs, ThreatEvaluation_AP/LE, Riskassessment_AP/LE*: Column for comments added * Sheet protection: configuration with as less as possible restrictions for the user
2.3.1/17.12.2018	Upgrade to 400 possible Damage Scenario/Threat pairs
2.3.2/04.12.2019	Residual Risk added as use case for this template

Methodology for Threat and Risk Analysis & Residual Risk Analysis

You can choose between two different approaches:

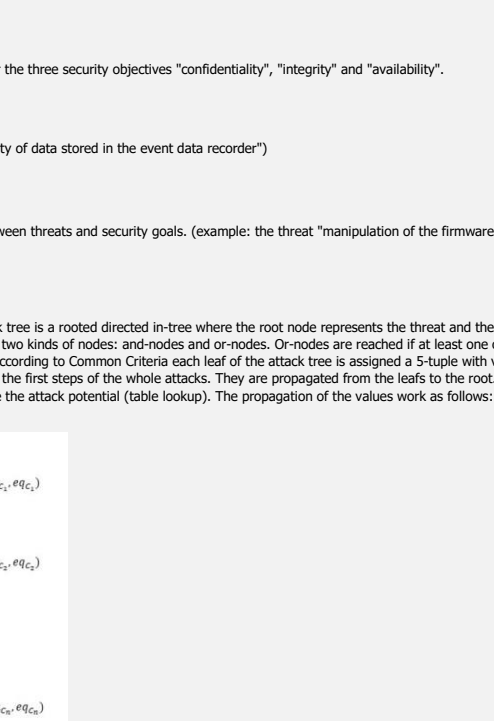
a) Threat and Risk Analysis using Attack Trees

1. Describe TOE
2. Optional: Collect misuse cases
3. Estimate consequences
   a. Identify damage scenarios
   b. For each damage scenario: estimate the consequence
4. Attack potential evaluation
   a. Identify all security assets
   b. Define relevant security goals by combining the security assets with the objectives confidentiality/integrity/ availability.
   c. Define threats: threat = non-fulfillment of security goal.
   d. For each threat: List the damage scenarios it could lead to.
   e. Calculate the attack potential by estimating time/expertise/knowledge/access/equipment which is necessary for the attack
5. For each damage scenario D: calculate $\mathrm{risk(D)} = \max_{T \to D} \frac{\mathrm{consequence(D)}}{\mathrm{attack\ potential\ (T)}}$
6. Derive security needs.



b) Threat and Risk Analysis with Likelihood Estimation

1. Describe TOE
2. Optional: Collect misuse cases
3. Estimate consequences
   a. Identify damage scenarios
   b. For each damage scenario: estimate the consequence
4. Likelihood estimation
   a. Identify all security assets
   b. Define relevant security goals by combining the security assets with the objectives confidentiality/integrity/ availability.
   c. Define threats: threat = non-fulfillment of security goal.
   d. For each threat: List the damage scenarios it could lead to.
   e. Estimate the likelihood for each theat.
5. For each damage scenario D: calculate $\mathrm{risk(D)} = consequence(D) \cdot \max_{T \to D} likelihood(T)$
6. Derive security needs.



Terms and Definitions

Misuse Case (MUC)

Once the TOE is defined the Security Manager gives a misuse case workshop where preferably all stakeholders of the product answer the question "What can go wrong with the TOE regarding security?". The answers to that question are called misuse cases (MUCs). Since the participants have different roles and backgrounds the MUCs have different technical and abstraction levels (examples: "kidnap passengers", "suppress safety reaction", "Install manipulated firmware"). However, these different perspectives help to avoid the effects of "operational blindness". As an additional positive aspect the workshop increases the security awareness in the project.

Damage Scenario

By a damage scenario we mean a scenario where a damage becomes directly perceptible to the user (e.g. driver) or to the Bosch Group (e.g. "personal damage", "privacy violation", "reputation damage to RB").

Consequence

The consequence describes the severity of a damage scenario. We consider the four consequences "negligible", "moderate", "serious" and "severe" characterized in Bosch Norm N103 SEC002.

Security Asset

A security asset is any data, function, or resource of the target of evaluation that should be protected. (example: "firmware", functionalities)

Security Objective

Security Objectives are used to clarify which aspects of a security asset need to be protected. We consider the three security objectives "confidentiality", "integrity" and "availability".

Security Goal

A security goal is the fulfillment of a security objective regarding a security asset. (example: "confidentiality of data stored in the event data recorder")

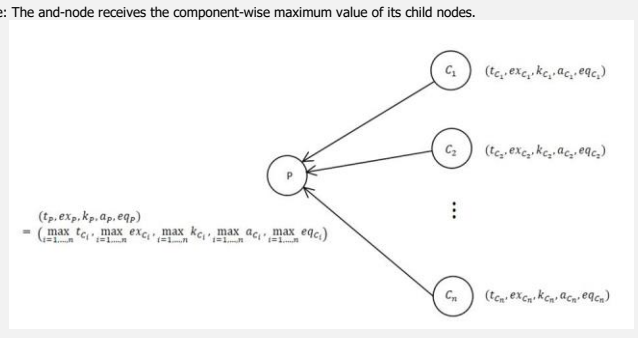
Threat

A threat is the non-fulfillment of a security objective for a security asset. Hence there is a 1:1-relation between threats and security goals. (example: the threat "manipulation of the firmware" affects the security goal "integrity of the firmware")

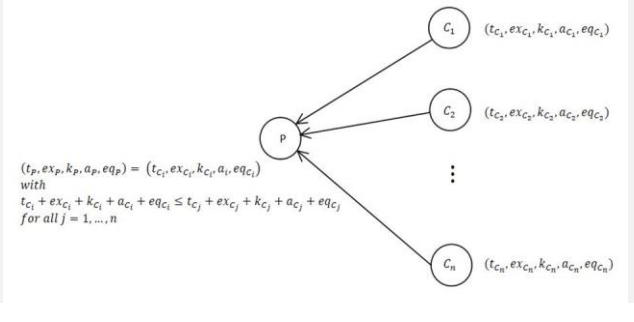
Attack Tree

For each threat we generate an attack tree describing all possible attacks that realize this threat. An attack tree is a rooted directed in-tree where the root node represents the threat and the child-nodes represent the single steps of the attacks that realize the threat. Depending on the structure of the attacks, there are two kinds of nodes: and-nodes and or-nodes. Or-nodes are reached if at least one of the attack steps represented by its child nodes is fulfilled. To reach an and-node all of its child nodes have to be fulfilled. According to Common Criteria each leaf of the attack tree is assigned a 5-tuple with values for elapsed time, expertise, knowledge, access and equipment. These values represent the effort for an attacker to perform the first steps of the whole attacks. They are propagated from the leafs to the root. The resulting 5-tuple represents the effort that is at least necessary to perform the attack. The sum of these 5 values determine the attack potential (table lookup). The propagation of the values work as follows:

• and-node: The and-node receives the component-wise maximum value of its child nodes.



• or-node:
- If the or-node is not followed by an and-node the or-node receives an arbitrary 5-tuple of its children with minimum sum over the 5 components.



- If there is an and-node following the or-node: in this case it is not clear from the sum of the five values which child yields the minimum sum in the root. Therefor the 5-tuples of all children needs to be tried out.

Attack Potential

The attack potential of a threat T is a value that indicates the minimum effort an attacker needs to make in order to realize this threat (see "Attack Tree"). We use the values "basic", "enhanced basic", "moderate", "high" and "beyond high" . The Attack potential is determined by

$$\min_{\substack{\text{attacks } A \\ \text{leading to } T}} (t_A + ex_A + kn_A + ac_A + eq_A)$$

Sum	Attack Potential
0-9	Basic
10-13	Enhanced Basic
14-19	Moderate
20-24	High
>25	Beyond High

Risk

For a damage scenario D and a threat T that leads to D the risk of (D,T) is defined as the expected loss when D happens caused by T.

$$R(D,T) = Consequence(D) \cdot \frac{1}{AttackPotential(T)} \text{ or}$$
$$R(D,T) = Consequence(D) \cdot Likelihood(T)$$

For a damage scenario D the risk of D is defined to be the maximum risk of D being caused by all possible threats T.

$$R(D) = \max_{T \text{ causing } D} R(D,T)$$

The multiplications Consequence · (1/Attack Potential) and Consequence · Likelihood are realized by table lookup:

Attack Potential	Risk Assessment			
Basic	Medium	High	Very High	Very High
Enhanced Basic	Medium	High	High	Very High
Moderate	Low	Medium	High	High
High	Low	Medium	Medium	High
Beyond High	Low	Low	Low	Medium
Consequence	Negligible	Moderate	Serious	Severe

Likelihood	Risk Assessment			
Highly Likely	Medium	High	High	Very High
Likely	Low	Medium	High	High
Less Likely	Low	Medium	Medium	High
Unlikely	Low	Low	Low	Medium
Consequence	Negligible	Moderate	Serious	Severe

Scaling Effect

By scaling effects we mean a significant increase in the expected damage accomplished by a relatively small increase in attack potential, or by a relatively small decrease in likelihood, respectively. (e.g. when the TOE is one product of a series and all products of the series have the same secret key, the effort of compromising the whole series is nearly the same as compromising just the TOE)

Security Need

A security need is a high level security requirement. Security needs follow from
- Threats identified in the TRA that lead to an unacceptable risk. (e.g. "R(crash, firmware manipulation)=High" yields the security need "secure firmware update functionality")
- Assumptions made for the TRA (e.g. the assumption "the in-vehicle communication is secure" yields the security need "secure in-vehicle communication".)
- Bosch or customer requirements (e.g. the OEM wants a special security mechanism to protect the OEM diagnosis interface)

4. Residual Risk Analysis (RRA)

The Residual Risk Analysis analyzes the risks once the Security Features specified in the Security Concept, designed to address the risks identified in the TRA, have been implemented. In practice, it is often convenient to start the RRA as a copy of the TRA and reassess the risks accordingly under the assumption that the Security Concept has been implemented.

Technical Description

Please describe the target of evaluation (TOE). Please include graphics describing the physical and logical architecture. If this TRA is an adaptation of a reference project TRA, please point out the differences.

Scope

Please describe the scope of the analysis. If this TRA is an adaptation of a reference project TRA, please point out the differences.

Assumptions

Please enter all assumptions made. If this TRA is an adaptation of a reference project TRA and there are changes regarding the assumptions, please make a comment.

Example

Assumption-ID	Assumptions	Comments
As-1	An attacker cannot break state-of-the-art cryptographic algorithms and protocols.	
As-2	The Robert Bosch software is trusted.	

Assumption-ID	Assumptions	Comments
As-1	Access to all unused physical interfaces in micro-controller are blocked.	NFC Interfaces
As-2	Attacker does not have physical access to the device	NFC Interface
As-3	Bosch insiders (e.g., personnel, developers, project managers and solution providers involved in this project) are trusted to the extent that they are authorized	Bosch responsibility
As-4	End user is adequately trained to use the tools as intended	BLE Interface/ Module
As-5	Physical security and safety of the devices deployed in the customer environment, including protection from physical tampering that may change any functionality and/or of the installation site is the responsibility of the customer.	Physical security and safety of the device must be ensured by customer. Physical access of devices must be monitored and controlled by

Comments

This sheet is optional. If you do not work with misuse cases please continue on the next sheet "DSsConsequences".

Misuse Cases

Please enter all relevant misuse cases (MUCs). If this TRA is an adaptation of a reference project TRA and there are changes regarding the MUCs, please make a comment.

Definition: A MUC is an answer to the general question "What can go wrong with the TOE concerning security?". Depending on the person who answers that question MUCs can vary in technical and abstraction levels.

Example

MUC-ID	MUC Description	Comment
MUC-1	The TOE sends manipulated messages over the CAN bus	
MUC-2	The attacker modifies the functionality of the TOE	
MUC-3	Cause an emergency braking	
MUC-4	Prevent the driver from taking over the vehicle's control	
MUC-5	Compromise backend in order to deliver manipulated information to the device	
MUC-6	Read out cryptographic material to bypass implemented security mechanisms	
MUC-7	Get unauthorized access to diagnostic services	
MUC-8	Read out DTCs in order to get private information about the driver's behavior	
MUC-9	Forging of maintenance data to support false claims	
MUC-10	Manipulate vehicle DTC for higher repair bill	
MUC-11	DoS of backend access by flooding wireless interfaces	
MUC-12	Send manipulated data from the backend to the device	
MUC-13	Extract the software in order to reverse engineer/ understand the device	
MUC-14	Do an unauthorized activation of a feature. This includes extensions (e.g. appstore) and built-in features which are disabled in the current model/ on the current platform	
MUC-15	Manipulation of HMI information to deceive the driver	
MUC-16	Flood internal connections with unusable data	
MUC-17	Send manipulated messages that have an impact on the vehicle's behavior	
MUC-18	Launch a replay attack of environment data	
MUC-19	Suppress sensor data before it is transmitted	
MUC-20	Store or forward privacy-relevant video data	
MUC-21	Manipulation of the vehicles state detection in order to disable functionality	

MUC-ID	MUC Description	Comment
MUC-1	WiFi / NFC may be misused to sniff (evesdrop) the communication between the device and paired mobile device	Insecure external interfaces
MUC-2	Cloning and misuse of NFC Card	NFC Card and Reader in eScooter
MUC-3	Cloning NFC Tags	NFC Tags
MUC-4	Entering into programming mode without authentication (by service tech NFC card)	NFC Reader
MUC-5	Manipulating parameter values in programming mode to save on milk or coffee beans to misuse the system	On-board NFC Reader, USB Interface
MUC-6	Manipulation of parameters to affect the quality through NFC or USB or UART	On-board NFC Reader, USB Interface, UART Interface
MUC-7	Reset the cup-count in case of a lost NFC Card	NFC Tags
MUC-8	Consuming memory by dumping large files through BLE communication	Maxing out limited on-board persistent memory
MUC-9	Service person loads undesirable content through BLE communication	Bluetooth Module
MUC-10	Evesdropping BLE communication	Insecure external BLE interfaces
MUC-11	Manipulate the firmware through OTA using Bluetooth	Firmware Update
MUC-12	Connecting to device from illegitimate mobile application	Device Bluetooth Stack
MUC-13	Sniffing the bluetooth communication between the device and mobile	Device and Mobile Aps
MUC-14	Access stored personal data in solution using BLE communication	Unauthorized Access
MUC-15	Cloning the database of by sniffing BLE communication	Due to unsecure BLE communication
MUC-16	An attacker hacks into the device via BLE to change the sensetive data	Hacking the solution via unsecure BLE comm.

Comments

Damage Scenarios and their Consequences

Please enter all relevant damage scenarios and assign the highest suitable consequence using the adjacent consequence classification. Please give reasons for the relevance of the damage scenario and for your choice of the specific consequence. If this TRA is an adaptation of a reference project TRA and there are changes regarding the damage scenarios or their consequences, please make a comment.

Example

DS-ID	Damage Scenario	Consequence	Reasoning for the relevance of the DS for this analysis	Reasoning for the choice of the consequence value	Comments
DS-1	Crash	Severe	MUC-1: An unreliable in-vehicle communication could affect the signals from the brake system ECU to the related actuators. This would mean a limitation of the braking functionality and could lead to a crash.	In a crash human safety could be severely affected leading to loss/losses of life.	

Remark: A crash can, for example, also cause costs (consequence "Negligible", "Moderate" or "Serious") or may have a negative impact on the confidence in RB (consequence "Serious"). But since we need to identify the highest suitable consequence these lower consequence are not considered further.

DS-2	Intellectual property is stolen	Serious	An attacker could disassemble the TOE and reverse engineer its firmware.	Since the TOE is highly innovative this would diminish the competitive edge of RB.	

Consequence Classification*

Consequence	Consequence Description
Severe	The consequences are not limited to Bosch. Causes loss of life, personal damages to many individuals and to society. • Human safety could be severely affected leading to loss/losses of life (AIS 5-6 – life threatening or deadly) • Critical infrastructure is adversely impacted • Massive misuse of personal data affecting a large number of individuals adversely • Damages are largely intangible. Cost-based consequence estimation is irrelevant
Serious	Considerable tangible or intangible damages to the Bosch Group; substantial loss of image or reputation • Human safety could be adversely affected (AIS 2-4 - causing injuries, passengers are injured, probably not life threatening) • Laws, regulations and contracts are violated leading to drastic legal consequences (e.g., criminal proceedings) and penalties • Customer confidence is violated • Competitive edge is diminished • Services are considerably affected for an indefinite period of time and it is impossible to maintain customer supplies or service level agreements (SLA's) • Potential cost of damage is very high (e.g. > 30 % annual sales of legal entity)
Moderate	Causes distinct negative consequences, impacts trust • Human safety could be lightly affected (AIS 1 – skin-deep wounds, muscle pains, ...) • Laws, regulations and contracts are violated leading to penalties • Trust of specific people, contracting partners, customers is adversely affected • Services are adversely affected resulting in reduction in scale of operations for a definite period of time • Potential cost of damage is high (e.g. 5 - 30 % annual sales of legal entity)
Negligible	Customers and business partners are inconvenienced. Time is lost in restoration activities. • Human safety is not affected (AIS 0) • Violation of laws, regulations and contracts are remediable • Customers or business partners are irritated and inconvenienced • Services are affected, but can be restored within a tolerable period of time • Potential cost of damage not very high (e.g. < 5% annual sales of legal entity)

* The Consequence Classes largely correspond to the ISO Impact Parameters.

DS-ID	Damage Scenario	Consequence	Reasoning for the relevance of the DS for this analysis	Reasoning for the choice of the consequence value	Comments
DS-1	Degradation or disruption or loss of functionality or unreliable operation	Moderate	There is a chance of functional or operational degradation due to manipulation	Services are affected but can be restored within a tolerable period of time	
DS-2	Disclosure of IP or Proprietary Data or sensitive Information, Unauthorized copying or	Moderate	Unauthorized reading of firmware or update may lead to IP disclosure	Research effort expended in developing Bosch IP is lost.	
DS-3	Misuse or manipulation affecting Bosch	Negligible	Manipulation of system data may lead to loss of revenue due to assertion of	Services are affected but can be restored within a tolerable period of time	
DS-4	Legal non-compliance	Serious	Compliance to legal requirements may be affected	Compliance to international and national legal requirements and standards	
DS-5	Loss of customer trust	Moderate	Customer trust/confidence is important for future business. For examole loss of	Trust of soecific people, partners are violated. which in turn affect the future	
DS-6	Degradation or disruption or loss of functionality or unreliable operation	Moderate	There is a chance of functional or operational degradation due to manipulation	Services are affected but can be restored within a tolerable period of time	
DS-7	Misuse or manipulation affecting Bosch	Negligible	Services are affected but can be restored within a tolerable period of time	Research effort expended in developing Bosch IP is lost.	
DS-8	Disclosure of Personally Identifiable Information	Moderate	Unauthorized reading of database or sniffing of communication may lead to	Compliance to international and national legal privacy requirements and	
DS-9	False claim affecting Bosch	Negligible	Financial loss	Potential cost of damage is not very high (< 5% of annual sales of legal	

Comments

Security Goals

Please enter all relevant assets and select their objectives. Please give a reason for your choices. If MUCs are identified this can be done by referencing the MUC that indicates the asset and its objective. Note that different MUCs can motivate the same asset and that MUCs can motivate multiple assets. If this TRA is an adaptation of a reference project TRA and there are changes regarding the security goals, please make a comment.

Definition: A security asset is any data, function, or resource of the target of evaluation (TOE) that should be protected.

Definition: A security goal is the fulfillment of a security objective regarding a security asset.

Example

Asset-ID	Asset Description	Objective	Description	Reasoning	Comments
A-1	in-vehicle communication	Integrity	The messages sent over the in-vehicle communication channels should be unalterable by an attacker. Furthermore it should not be possible to feed fake messages to the in-vehicle communication channels.	MUC-1	
A-1	in-vehicle communication	Availability	An attacker should not be able to suppress the transmission of messages.	Otherwise an attacker could suppress actuator messages and disable the braking functionality.	
A-2	firmware	Integrity	The firmware should be unalterable by an attacker.	MUC-2: Firmware manipulation could change the behavior and functionality of the TOE.	
A-2	firmware	Confidentiality	The attacker should not be able to read out the firmware.	The firmware of the TOE is highly innovative and needs to be kept secret.	

Asset-ID	Asset Description	Objective	Description	Reasoning	Comments
A-1	NFC Tags	Confidentiality	NFC card contains sensitive information like UID which should not be exposed.		
A-1	NFC Tags	Integrity	NFC card contains sensitive information like UID which should not be manipulated. Asset the		
A-2	NFC communication	Availability	NFC communication shall be protected by DDoS attack to prevent blocking or loss of		
A-3	NFC Reader	Availability	NFC Reader should be available to take the input fro NFC tag		
A-3	NFC Reader	Confidentiality	against NFC known attacks.		
A-4	BLE Module	Confidentiality	BLE security profile used for communication must be applicable to avoid BLE traffic from being		
A-5	BLE API	Confidentiality	BLE communication may expose sensitive information needed to access the system.		
A-5	BLE API	Integrity	BLE communication may be tampered by MITM attacks to affect performance.		
A-5	BLE API	Availability	Malicious entities may create one or more shared secret keys and the store these keys for use		
A-6	BLE Communication	Confidentiality	exploitare of BLE communication will expose information such as diagnostic information, user		
A-6	BLE Communication	Integrity	manipulation of BLE communication will lead to tampering of diagnostic values, firmware		
A-6	BLE Communication	Availability	Unavailability of BLE communication will lead to loss/degraded functionality.		

Comments

Threats and Possible Damage Scenarios

Please formulate the threats and decide for each threat to which damage scenarios it could lead. Please note that a threat can result in more than one damage scenario and that different threats can result in the same damage scenario. Please give reasons for your choices. If this TRA is an adaptation of a reference project TRA and there are changes regarding the threats, please make a comment.

Definition: A threat is the non-fulfillment of a security goal.

Example

Threat-ID	Threat	Affected Security Goal	DS-ID	Damage Scenarios	Reasoning	Comments
Th-1	Manipulation of in-vehicle communication	Integrity of in-vehicle communication	DS-1	Crash	The manipulation of sensor signals to the TOE or actuator messages from the TOE to the braking units could result in a crash.	
			DS-3	Functionality is limited or denied	When the TOE receives manipulated sensor signals the intended functionalities of the TOE are not triggered.	
			DS-4	Reputation damage	An unsafe vehicle containing a RB ECU means negative publicity for RB.	
Th-2	Manipulation of firmware	Integrity of firmware	DS-1	Crash	The firmware could be manipulated in a way that the TOE does not send the intended actuator messages to the steering or braking units.	
			DS-3	Functionality of the TOE is limited or denied	The functionalities of the TOE are defined by the TOE firmware.	
			DS-4	Reputation damage	An unsafe vehicle containing an RB ECU means negative publicity for RB.	
Th-3	Unauthorized reading of firmware	Confidentiality of firmware	DS-2	Intellectual property is stolen	The firmware is highly innovative.	

Threat-ID	Threat	Affected Security Goal	DS-ID	Damage Scenarios	Reasoning	Comments
Th-1	Extraction of NFC Tags	Confidentiality of NFC Tags	DS-2	Disclosure of IP or Proprietary Data or sensitive		
Th-2	Manipulation of NFC Tags	Integrity of NFC Tags	DS-3	Misuse or manipulation affecting Bosch		
Th-3	Blocking NFC communication	Availability of NFC communication	DS-1	Degradation or disruption or loss of functionality or		
Th-4	Blocking NFC Reader	Availability of NFC Reader	DS-1	Degradation or disruption or loss of functionality or		
Th-5	Extraction of NFC Reader	Confidentiality of NFC Reader	DS-4	Legal non-compliance		
Th-6	Extraction of BLE Module	Confidentiality of BLE Module	DS-9	False claim affecting Bosch		
Th-7	Extraction of BLE API	Confidentiality of BLE API	DS-8	Disclosure of Personally Identifiable Information		
Th-8	Manipulation of BLE API	Integrity of BLE API	DS-1	Degradation or disruption or loss of functionality or		
Th-9	Blocking BLE API	Availability of BLE API	DS-5	Loss of customer trust		
Th-10	Extraction of BLE Communication	Confidentiality of BLE Communication	DS-8	Disclosure of Personally Identifiable Information		
Th-11	Manipulation of BLE Communication	Integrity of BLE Communication	DS-3	Misuse or manipulation affecting Bosch		
Th-12	Blocking BLE Communication	Availability of BLE Communication	DS-1	Degradation or disruption or loss of functionality or		

Comments

Evaluation of Threats using Attack Potential

Please create an attack tree for each of the identified threats and describe possible scaling effects of the threats. If this TRA is an adaptation of a reference project TRA and there are changes regarding the attack potentials of the threats, please make a brief comment here and explain the details on the sheet AttackTrees.

Example

Tree-ID	Technical Attack Tree	Attack Potential					Sum	Attack Potential	Path to Technical Attack Tree	Scaling Effects	Comments
		T	E	K	A	Eq					
Tr-1	Enter CAN bus via OBD II interface	2	3	0	5	0	10	Enhanced Basic	C:\AttackTrees\TAT-OBDII.vsdm	None as physical access to the individual vehicle is necessary.	

Threat-ID	Threat	Attack Potential					Sum	Attack Potential	Path to Attack Tree	Scaling Effects	Comments
		T	E	K	A	Eq					
Th-2	Manipulation of firmware	4	3	0	5	1	13	Enhanced Basic	C:\AttackTrees\FirmwareManipulation.vsdm	An attacker needs to extract/analyze the firmware (effort (4,3,0,0,1)), implement changes (effort (1,3,0,0,0)) and manipulate the flash memory (effort for one vehicle (4,3,0,5,0) via access to the external memory). By misusing the FOTA flashing procedure, the attacker can compromise the whole fleet since all instances of the TOE use the same cryptographic keys (effort for flash manipulation of the whole fleet (19,3,0,0,4)).	

Attack Potential Values

Value	Factor	Comment
	Elapsed Time	Is the total amount of time taken by an attacker to identify that a particular potential vulnerability may exist in the product, to develop an attack method and to sustain effort required to mount the attack against the product. When considering this factor, the worst case scenario is used to estimate the amount of time required.
0	<= one day	
1	<= one week	
2	<= two weeks	
4	<= one month	
7	<= two months	
10	<= three months	
13	<= four months	
15	<= five months	
17	<= six months	
19	> six months	
	Expertise	Refers to the level of generic knowledge of the underlying principles, product type or attack methods (e.g. Internet protocols, Unix operating systems, buffer overflows).
0	Layman	Laymen are unknowledgeable compared to experts or proficient persons, with no particular expertise.
3	Proficient	Proficient persons are knowledgeable in that they are familiar with the security behavior of the product or system type. When several proficient persons are required to complete the attack path, the resulting level of expertise still remains "proficient" (which leads to a 3 rating).
6	Expert	Experts are familiar with the underlying algorithms, protocols, hardware, structures, security behavior, principles and concepts of security employed, techniques and tools for the definition of new attacks, cryptography, classical attacks for the product type, attack methods, etc. implemented in the product or system type.
8	Multiple Experts	The level "Multiple Expert" is introduced to allow for a situation, where different fields of expertise are required at an Expert level for distinct steps of an attack.
	Knowledge of Product	Refers to specific expertise in relation to the product. This is distinct from generic expertise, but not unrelated to it.
0	Public	Public information concerning the product (e.g. as gained from the Internet).
3	Restricted	Restricted information concerning the product (e.g. knowledge that is controlled within the developer organization and shared with other organizations under a non-disclosure agreement).
7	Sensitive	Sensitive information about the product (e.g. knowledge that is shared between discreet teams within the developer organization, access to which is constrained only to members of the specified teams).
11	Critical	Critical information about the product (e.g. knowledge that is known by only a few individuals, access to which is very tightly controlled on a strict need to know basis and individual undertaking).
	Access (Window of Opportunity)	Is also an important consideration, and has a relationship to the Elapsed Time factor. Identification or exploitation of a vulnerability may require considerable amounts of access to a product that may increase the likelihood of detection. Some attack methods may require considerable effort off-line, and only brief access to the product to exploit. Access may also need to be continuous, or over a number of sessions. For some products the Window of opportunity may equate to the number of samples of the product that the attacker can obtain. This is particularly relevant where attempts to penetrate the product may result in the destruction of the product preventing use of that product sample for further testing, e.g. hardware devices. Often in these cases distribution of the product is controlled and so the attacker must apply effort to obtain further samples of the product.
0	Remote and unlimited	Logical or remote access without physical presence, for instance, wireless or via Internet, e.g. V2X or cellular interface or IT back-end. Also the attack doesn't need any kind of opportunity to be carried because there is no risk of being detected during the attack.
2	Remote and limited	Logical or remote access without physical presence but the window of opportunity is limited due to a potential detection or target is only exposed for a limited time frame.
5	Easy Physical access	Simple physical access is sufficient for the attack.
7	Medium Physical access	Complex disassembly to access deep internals, e.g. direct flash memory access. However without breaking sophisticated tamper-protection boundaries, e.g. more than special screws and similar "unsophisticated" measures
11	Difficult Physical access	Disassembly on microelectronic level, e.g. micro probing/cutting, chemistry, including breaking some sophisticated tamper-protection boundaries
	Equipment	Refers to the equipment required to identify or exploit a vulnerability.
0	Standard	Standard equipment is readily available to the attacker, either for the identification of a vulnerability or for an attack. This equipment may be a part of the product itself (e.g. a debugger in an operating system), or can be readily obtained (e.g. Internet downloads, protocol analyzer or simple attack scripts).
4	Specialized	Specialized equipment is not readily available to the attacker, but could be acquired without undue effort. This could include purchase of moderate amounts of equipment (e.g. power analysis tools, use of hundreds of PCs linked across the Internet would fall into this category), or development of more extensive attack scripts or programs. If clearly different test benches consisting of specialized equipment are required for distinct steps of an attack this would be rated as bespoke. If clearly different test benches consisting of specialized equipment are required for distinct steps of an attack, this should be rated as bespoke.
7	Bespoke	Bespoke equipment is not readily available to the public as it may need to be specially produced (e.g. very sophisticated software), or because the equipment is so specialized that its distribution is controlled, possibly even restricted. Alternatively, the equipment may be very expensive.
9	Multiple bespoke	The level "Multiple Bespoke" is introduced to allow for a situation, where different types of bespoke equipment are required for distinct steps of an attack.

Threat-ID	Threat	Attack Potential					Sum	Attack Potential	Path to Attack Tree	Scaling Effects	Comments
		T	Ex	K	A	Eq					
Th-1	Extraction of NFC Tags										
Th-2	Manipulation of NFC Tags										
Th-3	Blocking NFC communication										
Th-4	Blocking NFC Reader										
Th-5	Extraction of NFC Reader										
Th-6	Extraction of BLE Module										
Th-7	Extraction of BLE API										
Th-8	Manipulation of BLE API										
Th-9	Blocking BLE API										
Th-10	Extraction of BLE Communication										
Th-11	Manipulation of BLE Communication										
Th-12	Blocking BLE Communication										

Comments

Attack Trees

Please insert pictures/graphics of the attack trees if you do not provide links to external attack tree files in the sheet ThreatEvaluation_AP. You can also use this sheet to provide additional information about the attack trees, e.g. when this TRA is an adaptation of a reference project TRA and there are changes regarding the attack trees. For simplicity and clarity you may create so-called technical attack tree. A technical attack tree is an attack tree that does not represent a threat but occurs as a branch in one or more attack trees.

Risk Assessment Using Attack Potential

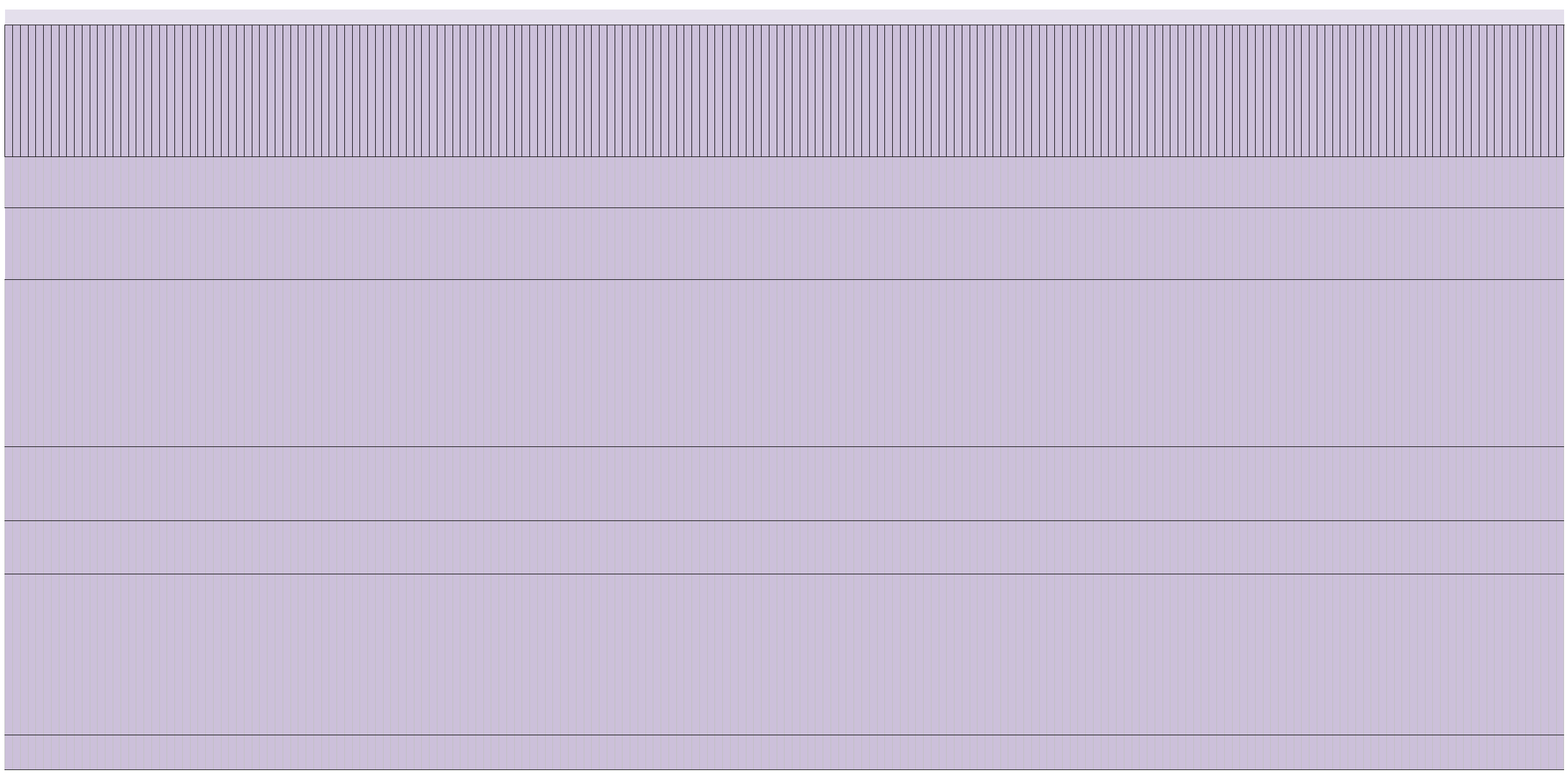
If this TRA is an adaptation of a reference project TRA and there are changes regarding the risks, please make a comment.

Example

Risk-ID	Damage Scenario (D)	Risk of D	Consequence of D	Threats T causing the Damage Scenario D	Attack Potential of T	Risk of (D,T)	Comments
R-1	Crash	Very High	Severe	Manipulation of in-vehicle communication	Basic	Very High	
R-2				Manipulation of firmware	Enhanced Basic	Very High	

Risk-ID	Damage Scenario (D)	Risk of D	Consequence of D	Threats T causing the Damage Scenario D	Attack Potential of T	Risk of (D,T)	Comments
R-1	Degradation or disruption or loss of functionality or		Moderate	Blocking NFC communication			
R-2				Blocking NFC Reader			
R-3				Manipulation of BLE API			
R-4				Blocking BLE Communication			
R-5	Disclosure of IP or Proprietary Data or sensitive Information,		Moderate	Extraction of NFC Tags			
R-6	Disclosure of Personally Identifiable Information		Moderate	Extraction of BLE API			
R-7				Extraction of BLE Communication			
R-8	False claim affecting Bosch		Negligible	Extraction of BLE Module			
R-9	Legal non-compliance		Serious	Extraction of NFC Reader			
R-10	Loss of customer trust		Moderate	Blocking BLE API			
R-11	Misuse or manipulation affecting Bosch		Negligible	Manipulation of NFC Tags			
R-12				Manipulation of BLE Communication			

Comments



Security Needs from TRA using Attack Potential

Please formulate and justify the security needs and select the responsible. If this TRA is an adaptation of a reference project TRA and there are changes regarding the security needs, please make a comment.

Example 1) Security Needs to cover the Assumptions

SN-ID	Security Need Description	Assumption	Comment	Responsible
SN-A-1	Only state-of-the-art cryptographic algorithms and protocols shall be used.	An attacker cannot break state-of-the-art cryptographic algorithms and protocols.	Otherwise an attacker can circumvent the implemented security mechanisms easily.	RB, OEM

Example 2) Security Needs to meet Bosch, Customer or other requirements

SN-ID	Security Need Description	Requirement	Comment	Responsible
SN-Rq-1	The OEM security mechanism for the diagnosis interface shall be implemented, provided that it is state-of-the-art.	The TOE shall include a diagnosis interface with a security mechanism for access control specified by the OEM.	OEM requirements should be fulfilled if possible. The restriction that the mechanism needs to be state-of-the-art is necessary to fulfill SN-A-1.	RB

Example 3) Security Needs arising from the Threats

SN-ID	Security Need Description	Threat T	Threat-ID	max. Risk caused by T	Comment	Responsible
SN-R-1	The diagnosis interfaces need to be protected against unauthorized access.	Manipulation of the firmware	Th-2	Very High	Accessing the diagnosis interface the firmware can be altered easilly.	RB, OEM

1) Security Needs to cover the Assumptions

SN-ID	Security Need Description	Assumption	Comment	Responsible	Comments

2) Security Needs to meet Bosch, customer or other requirements

SN-ID	Security Need Description	Requirement	Comment	Responsible	Comments

3) Security Needs arising from the Threats

SN-ID	Security Need Description	Threat T	Threat-ID	max. Risk caused by T	Comment	Responsible	Comments
SN-R-1	Higher-security products for NFC authentication, encryption and integrity checks must be used.	Extraction of NFC Tags	Th-1				
SN-R-2	System specific analytics data shall be protected from unauthorized access or exposure.	Extraction of NFC Tags	Th-1				
SN-R-3	USB Interface shall be protected against unauthorized access - physical and logical controls are required to	Extraction of NFC Reader	Th-5				
SN-R-4	Sensitive information like UID being read by TCU from eScooter NFC Reader shall be protected against	Manipulation of NFC Tags	Th-2				
SN-R-5	Sensitive information like UID in NFC Card shall be protected against reading out when swiping at Main	Blocking NFC communication	Th-3				
SN-R-6	The NFC Card at Main Station shall be protected against physical theft	Blocking NFC Reader	Th-4				
SN-R-7	Access to all unused BLE physical interfaces in micro-controller are blocked.	Extraction of BLE Module	Th-6				
SN-R-8	BLE communication shall be encrypted	Extraction of BLE Communication	Th-10				
SN-R-9	Third party software / libraries / API are trusted and are compatible, that is, when integrated with the TOE do	Extraction of BLE API	Th-7				
SN-R-10	Diagnosis will be performed only through trusted hardware an trustworthy personal	Extraction of BLE Module	Th-6				
SN-R-11	BLE shall be protected against unauthorized access. Latest version of BLE shall be implemented which	Extraction of BLE Communication	Th-10				
SN-R-12	User authentication shall be built into the BLE application to enable service level authentication	Blocking BLE Communication	Th-12				
SN-R-13	BLE communication shall be protected against DoS attacks	Blocking BLE Communication	Th-12				
SN-R-14	BLE communication shall check for authenticity	Extraction of BLE Communication	Th-10				
SN-R-15	BLE communication shall have integrity check	Manipulation of BLE Communication	Th-11				
SN-R-16	BLE communication shall use mutual authentication	Extraction of BLE API	Th-7				
SN-R-17	BLE messages in advertisement channel shall be digitally signed	Extraction of BLE Communication	Th-10				
SN-R-18	BLE services shall perform input validation	Manipulation of BLE Communication	Th-11				
SN-R-19	Firmware shall be protected against exposure.	Extraction of BLE Communication	Th-10				
SN-R-20	Flash memory contents shall be protected from unauthorized reading out.	Manipulation of BLE Communication	Th-11				
SN-R-21	For pairing with devices having BLE version later than 4.1 Security Mode 4 Level 4 shall be employed. For	Extraction of BLE API	Th-7				
SN-R-22	Link keys shall be unique and random and not static and shall not be reused for every pairing otherwise they	Extraction of BLE API	Th-7				

Management Summary of TRA / RRA using Attack Potential

Please write a management summary and summarize possible scaling effects of the threats leading to the related damage scenario in the table below. If this TRA is an adaptation of a reference project TRA, please mention the differences regarding security.

Results of the Risk Assessment

Damage Scenario	Risk	Scaling Effects	Comments
Degradation or disruption or loss of functionality or unreliable operation			
Disclosure of IP or Proprietary Data or sensitive Information, Unauthorized copying or cloning,			
Misuse or manipulation affecting Bosch			
Legal non-compliance			
Loss of customer trust			
Degradation or disruption or loss of functionality or unreliable operation			
Misuse or manipulation affecting Bosch			
Disclosure of Personally Identifiable Information			
False claim affecting Bosch			
