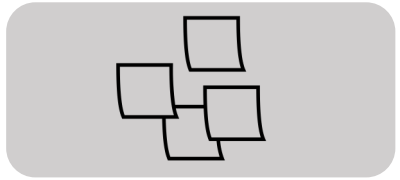
On the Secure and Resilient Design of Connected Vehicles: Methods and Guidelines

Thomas Rosenstatter

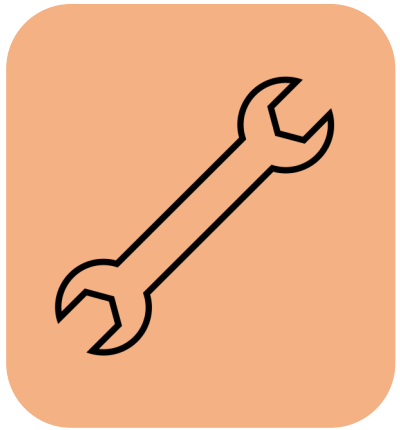
PhD Defense 14/10/21

Chalmers University of Technolgy



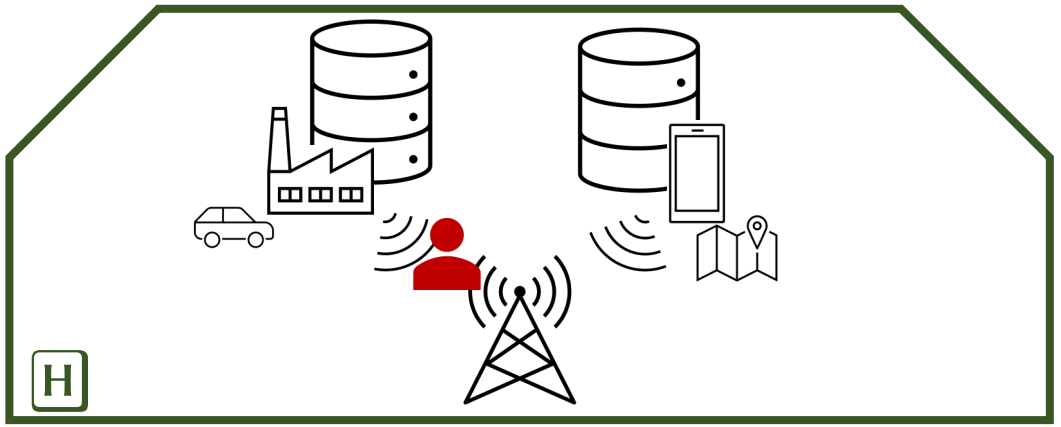
Part I. Introduction

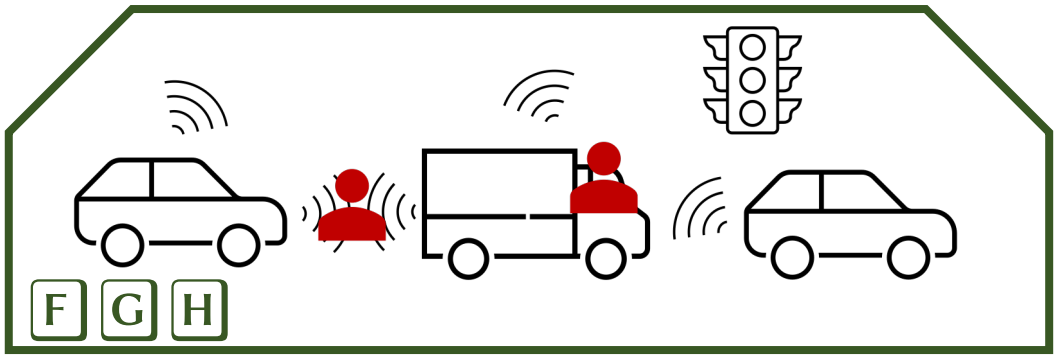
Part II. Generic Security Requirements and Identification of Suitable Techniques

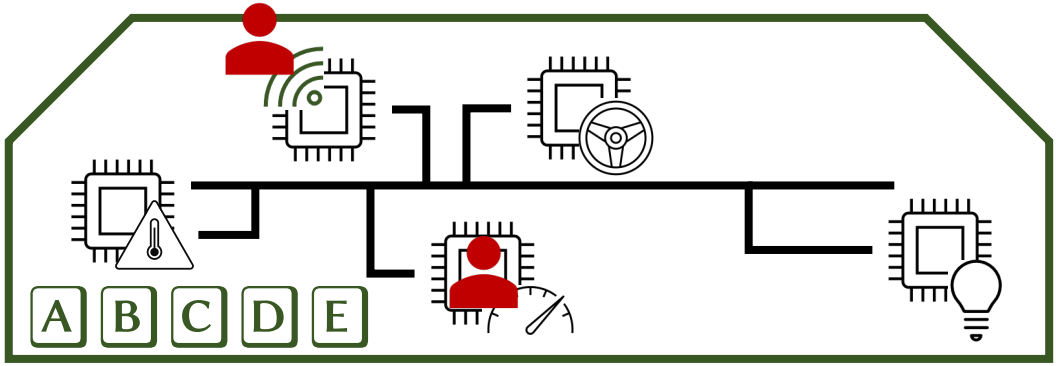


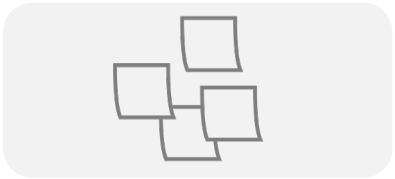
Part III. Design and Evaluation of Security and Resilience Techniques

AUTOMOTIVE SYSTEMS





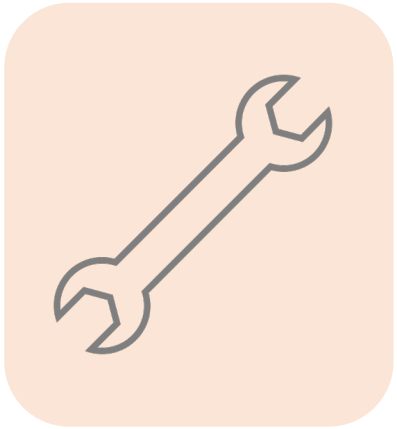




Part I. Introduction

Part II. Generic Security Requirements and Identification of Suitable Techniques

- A B Linking security demands to generic security requirements
- C Taxonomy for resilience techniques
- D Resilience and security techniques based on analysing disclosed attacks



Part III. Design and Evaluation of Security and Resilience Techniques

Requirements and Techniques

Aim:

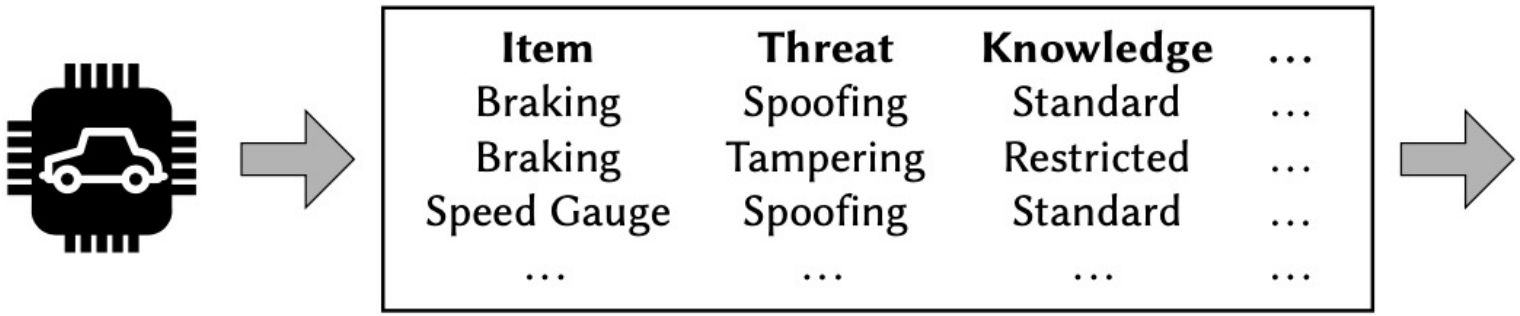
Support and guide developers in choosing appropriate security requirements and techniques for the task at hand.

Method:

- A B Analysis of existing standards for safety and ***security*** from other domains and proposed automotive security frameworks
- C Literature review of ***resilience*** techniques and taxonomies
- D Security assessment of disclosed attacks

Example

TARA



Item	Threat	Knowledge	…
Braking	Spoofing	Standard	…
Braking	Tampering	Restricted	…
Speed Gauge	Spoofing	Standard	…
…	…	…	…

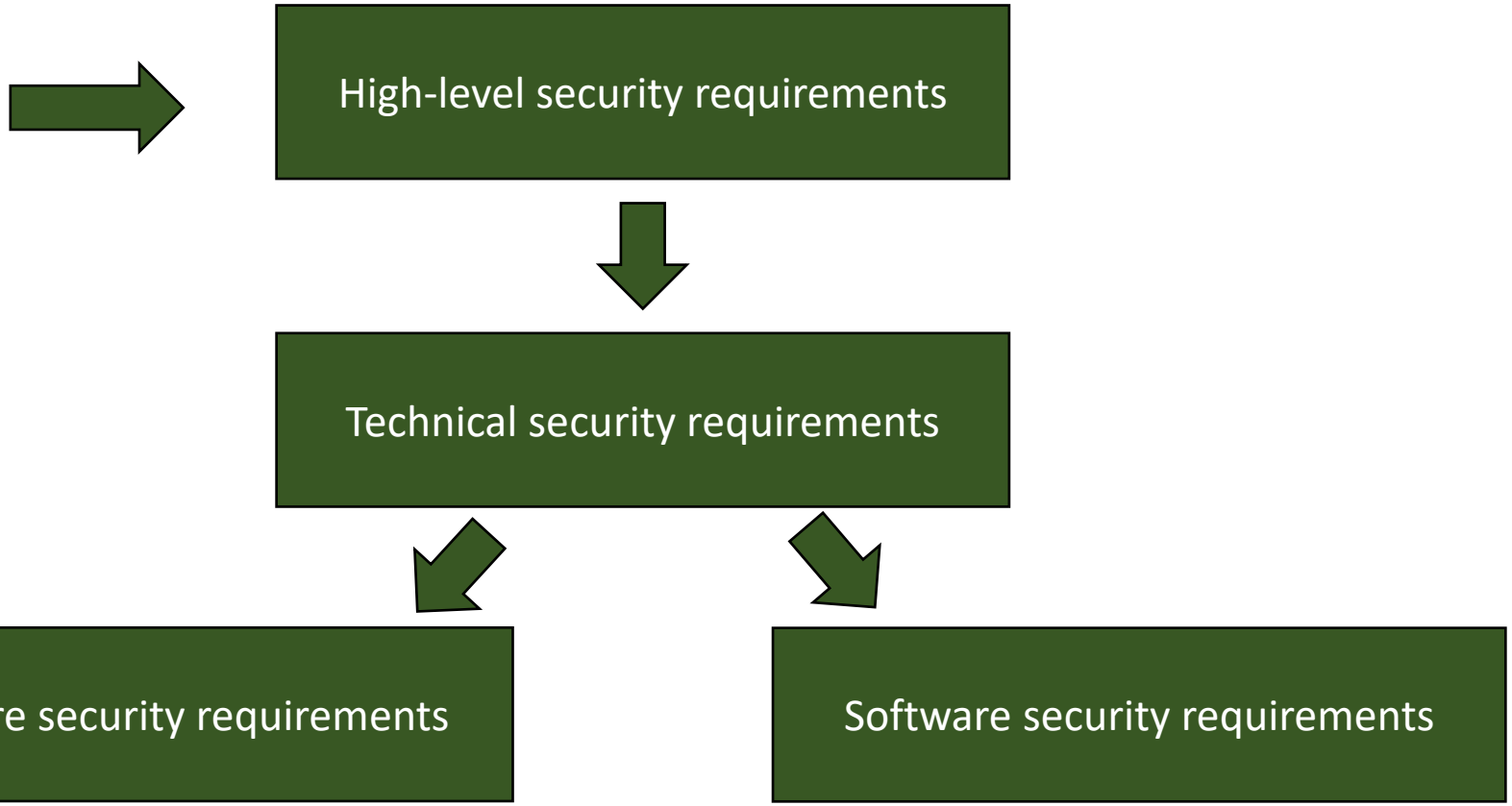
Classification

Security Level
3

Example: HEAVENS

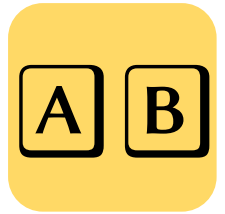
Classification

Asset/Item	Threat	Security Level
Speed	Spoofing	3
Speed	Information Disclosure	1



*According to HEAVENS risk assessment framework (*Islam, Lautenbach, Sandberg, Olovsson 2016*)

Mapping of Security Levels to Generic Requirements



Classification

$$\begin{bmatrix} Authenticity \\ Integrity \\ Non-repudiation \\ Confidentiality \\ Availability \\ Authorisation \end{bmatrix} = \begin{bmatrix} 3 \\ 3 \\ 2 \\ 1 \\ 3 \\ 2 \end{bmatrix}$$

Selection of security mechanisms

	SL 1	SL 2	SL 3	SL 4
Authenticity				
Message auth.			•	•
Firmware auth.	•	•	•	•
Hardware auth.				•

Cybersecurity goals

Based on an analysis of existing standards for safety and security from other domains and proposed automotive security frameworks

Safety Requirements

Cybersecurity requirements

[A] T. Rosenstatter and T. Olovsson, "*Open Problems when Mapping Automotive Security Levels to System Requirements*", VEHITS 2018

[B] T. Rosenstatter and T. Olovsson, "*Towards a Standardized Mapping from Automotive Security Levels to Security Mechanisms*", ITS-C 2018

		SL 0	SL 1	SL 2	SL 3	SL 4
Integrity	IN.1 [MSG] Message Authentication Code (MAC) with pre-shared key			•	•	•
	IN.2 [FW] Verify cryptographic hash of firmware when upgrading		•	•	•	•
	IN.3 [FW] Verify cryptographic hash of firmware/functions on boot				•	•
	IN.4 [HW] Physical protection against tampering				•	•
	IN.5 [HW] Detection of physical tampering		•	•	•	•
Authenticity	AU.1 [MSG] Message Authentication Code (MAC) with session key				•	•
	AU.2 [FW] Verify authenticity of firmware when upgrading using digital signatures[a]		1	1	2	2
	AU.3 [FW] Verify authenticity of firmware/functions on boot using digital signatures[a]				1	2
	AU.4 [HW] Verify hardware authenticity					•
Non-repudiation	NR.1 [MSG] Freshness using counter or timestamp in authenticated message				•	•
	NR.2 [MSG] Audit logging				•	•
	NR.3 [MSG] Use of digital signatures for messages (signals)					•
Confidentiality	CO.1 [MSG] Encryption of messages				•	•
	CO.2 [FW] Encryption of firmware during transmission[a]				1	2
Availability	AV.1 [MSG] Limited network access – Quality of Service				•	•
	AV.2 [FW] Watchdog timer			•	•	•
Authorization and Access Control	AC.1 [MSG] Whitelisting of messages (signals) on gateways		•	•	•	•
	AC.2 [MSG] Whitelisting of messages (signals) on nodes				•	•
	AC.3 [MSG] Access control on function level				•	•
	AC.4 [MSG] Deployment of Intrusion Detection Systems				•	•
	AC.5 [MSG, FW, HW] Logical separation[a]			1	1	2
	AC.6 [MSG, FW, HW] Domain isolation				•	•
Other requirements[b]	OR.1 Fail in known state					
	OR.2 Information Input Validation					
	OR.3 Operate with least set of privileges that are necessary					
	OR.4 Compliance to secure coding guidelines					
	OR.5 Secure Logging					

Verified with a vehicle manufacturer

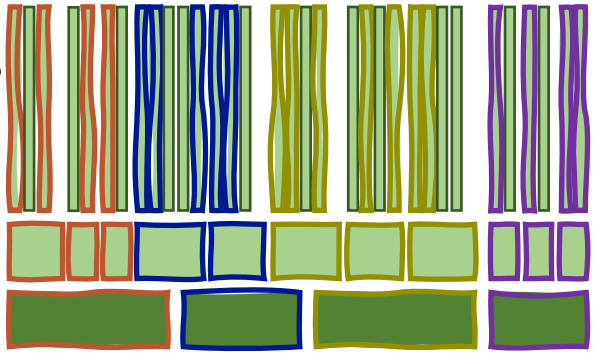
REMIND Resilience Techniques

Query scopus database

Manual review of **200** most relevant publications returned by scopus

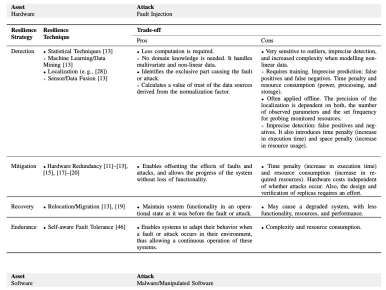
12 publications

Taxonomy



Collection and classification of identified techniques in taxonomy

Guidelines

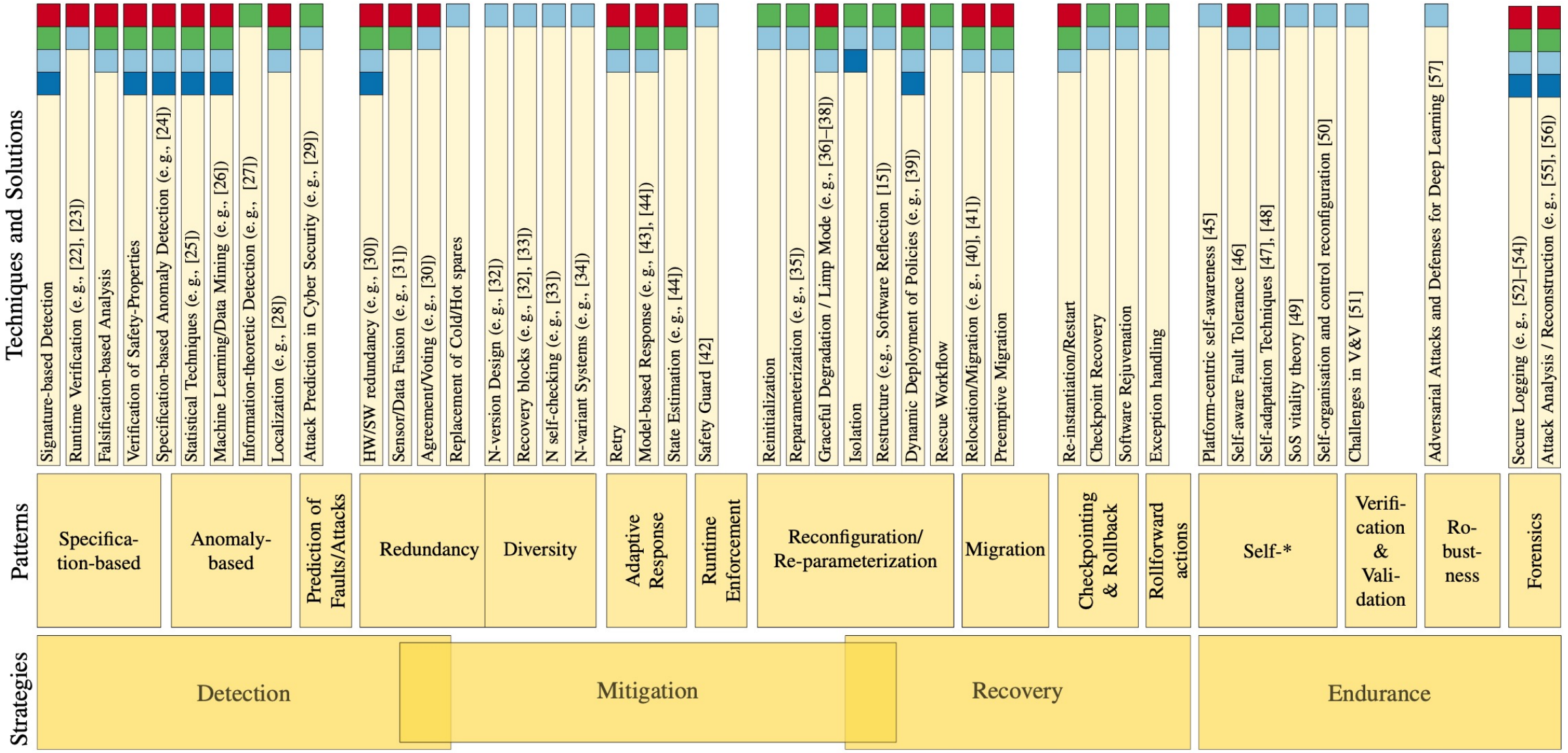


Asset		Attack	
Hardware		Fault Injection	
Resilience Strategy	**Resilience Technique**	**Trade-off**	
		Pros	Cons
Detection	• Statistical Techniques [13] • Machine Learning/Data Mining [13] • Localization (e.g., [28]) - Sensor/Data Fusion [13]	• Less computation is required. • No domain knowledge is needed. It handles multivariate and non-linear data. • Identifies the exclusive part causing the fault or attack. • Calculates a value of trust of the data sources derived from the normalization factor.	• Very sensitive to outliers, imprecise detection, and increased complexity when modelling non-linear data. - Requires training. Imprecise prediction: false positives and false negatives. Time penalty and resource consumption (power, processing, and storage). • Often applied offline. The precision of the localization is dependent on both, the number of observed parameters and the set frequency for probing monitored resources. - Imprecise detection: false positives and negatives. It also introduces time penalty (increase in execution time) and space penalty (increase in resource usage).
Mitigation	• Hardware Redundancy [11]–[13], [15], [17]–[20]	• Enables offsetting the effects of faults and attacks, and allows the progress of the system without loss of functionality.	• Time penalty (increase in execution time) and resource consumption (increase in required resources). Hardware costs independent of whether attacks occur. Also, the design and verification of replicas requires an effort.
Recovery	• Relocation/Migration [13], [19]	• Maintain system functionality in an operational state as it was before the fault or attack.	• May cause a degraded system, with less functionality, resources, and performance.
Endurance	• Self-aware Fault Tolerance [46]	• Enables systems to adapt their behavior when a fault or attack occurs in their environment, thus allowing a continuous operation of these systems.	• Complexity and resource consumption.
Asset		Attack	
Software		Malware/Manipulated Software	

Guidelines to show how these techniques can be combined

© T. Rosenstatter, K. Strandberg, R. Jolak, R. Scandariato and T. Olovsson, "*REMIND: A Framework for the Resilient Design of Automotive Systems*", SecDev 2020

REMIND Resilience Techniques



Resilient Shield

52 disclosed attacks

Security analysis according to SPMT methodology

[Strandberg2018Securing]

37 high and critical risk attacks

Assets	Potential threat actors	STRIDE categories	Security/resilience techniques
Hardware			
sensor:came			
Communicat			
internal:can			
Software			
running:firm…			
Data Storage			
crypto:certificate			

[D] K. Strandberg, T. Rosenstatter, R. Jolak, N. Nowdehi and T. Olovsson, "*Resilient Shield: Reinforcing the Resilience of Vehicles against Security Threats*", VTC2021-Spring

Resilient Shield

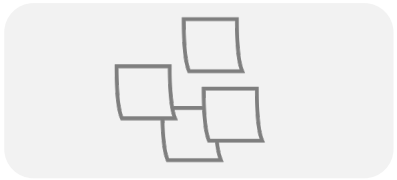
Assets targeted by attacks with high or critical risk.
ToE category:subcategory reference

■ Resilience patterns identified in REMIND [18]

Potential Threat Actors
Financial Actor (FA)
Foreign Country (FC)
Cyber Terrorist (CT)
Insider (IN)
Hacktivist (HA)
Script Kiddie (SK)

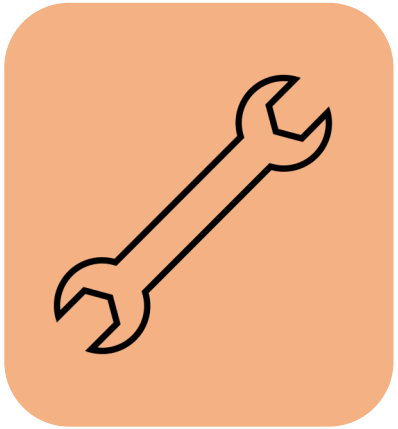
STRIDE categories
(S)poofing
(T)ampering
(R)epudiation
(I)nformation Disclosure
(D)enial of service
(E)levation of privilege

			(SG.1,8) Authentication	(SG.1) Encryption	(SG.2) Redundancy/Diversity ■	(SG.3) Access Control	(SG.3) Runtime Enforcement ■	(SG.4,8) Secure Storage	(SG.4) Secure Boot	(SG.4) Secure Programming	(SG.4) Secure Software Update	(SG.4) Verification & Validation ■	(SG.5) Separation ■	(SG.6) Specification-based Detection ■	(SG.6) Anomaly-based Detection ■	(SG.6) Prediction of Faults/Attacks ■	(SG.6) Adaptive Response ■	(SG.6) Reconfiguration ■	(SG.6) Migration ■	(SG.6) Checkpoint & Rollback ■	(SG.6) Rollforward actions ■	(SG.7) Self-X ■	(SG.7) Robustness ■	(SG.8) Forensics ■
Hardware																								
sensor:camera [34], [35]	FC, CT, HA	S, D			•												•	•				•	•	
sensor:GNSS [24], [26], [29], [30], [32]	FC, CT, HA	S	•		•										•		•	•				•	•	
sensor:lidar [28], [34]	FC, CT, HA	S, D			•												•	•				•	•	
sensor:ultrasonic [35]	FC, CT, HA	S, D			•												•	•				•	•	
Communication																								
internal:can [40], [44], [46], [47], [49]	FA, FC, CT, IN, HA	S, T, I, D	•	•	•	•	•						•	•	•	•		•	•			•		•
internal:flexray [37]	FA, FC, CT, HA	S, D	•			•	•						•	•	•			•				•		•
external:bluetooth [4], [36]	FC, CT, HA	S, T, D, E	•			•							•											
external:usb [4]	FC, CT, HA	S, T, E	•			•							•											
external:keyfob [22], [23]	HA, SK	S	•			•									•								•	
external:wifi [5], [33]	HA, SK	S, I	•	•		•				•			•											
external:cellular [3], [4], [41], [45], [51], [52]	FC, CT, HA, SK	S, T, I, D, E	•			•							•											
external:obdII [7], [27], [31], [38], [40], [43], [46], [48]	CT, HA	S, T, I, D, E	•			•	•						•	•	•			•		•		•		•
external:debugport [3], [41]	HA, IN	I, E	•			•																		
Software																								
running:state [25]	FC, CT, HA	S, D				•				•				•	•					•	•			•
running:firmware [3]–[5], [33], [36], [39], [41], [45], [51], [52]	FC, CT, HA	S, T, E				•				•	•	•	•	•	•			•				•		•
instorage:update [4], [36], [41]	HA, SK	S, T, E	•	•		•		•	•		•		•	•	•	•	•	•	•					•
instorage:weakcrypto [21], [50], [52]	FC, CT, HA, SK	S, E	•							•													•	
Data Storage																								
crypto:certificates [41]	FC, CT, HA	I		•		•		•	•															
hw:replaced [42]	HA, SK	I	•	•		•																		



Part I. Introduction

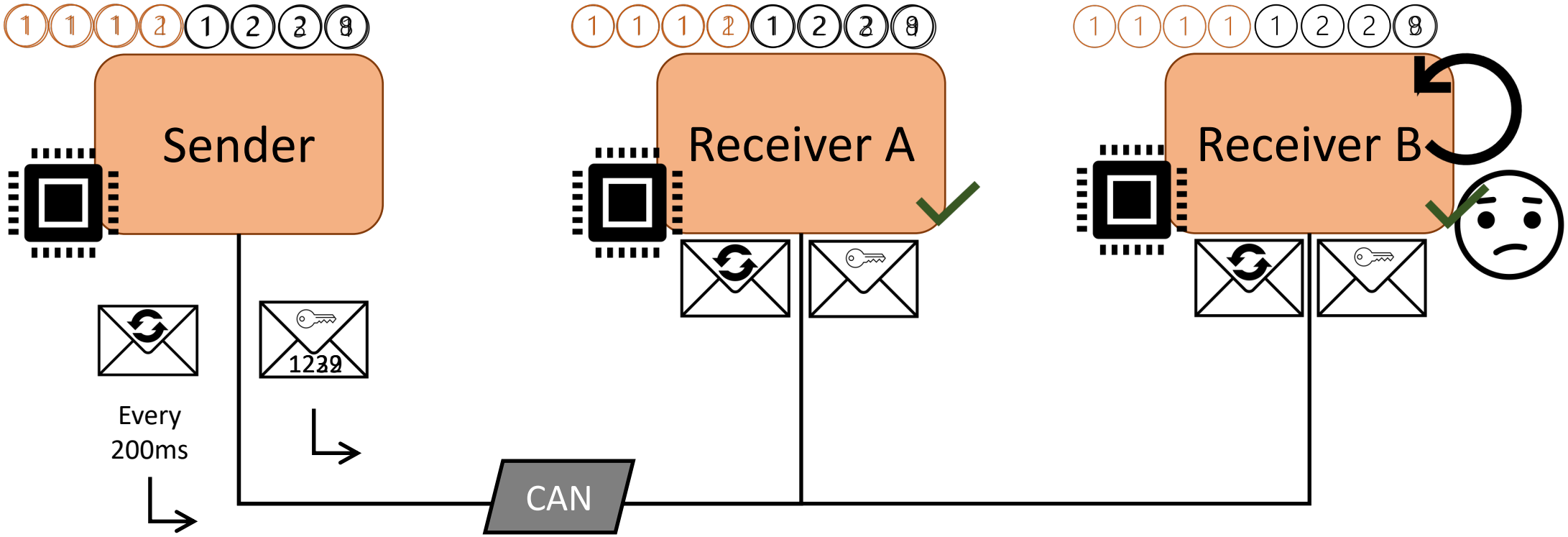
Part II. Generic Security Requirements and Identification of Suitable Techniques



Part III. Design and Evaluation of Security and Resilience Techniques

- E — Extension of a freshness mechanism
- F G — A trust model for cooperative vehicles
- H — Anomaly detection framework using Trust

Extension of AUTOSAR SecOC Profile 3



Detailed Analysis for Recovery + Simplified FV

Trade-off Analysis (local vs centralised manager)

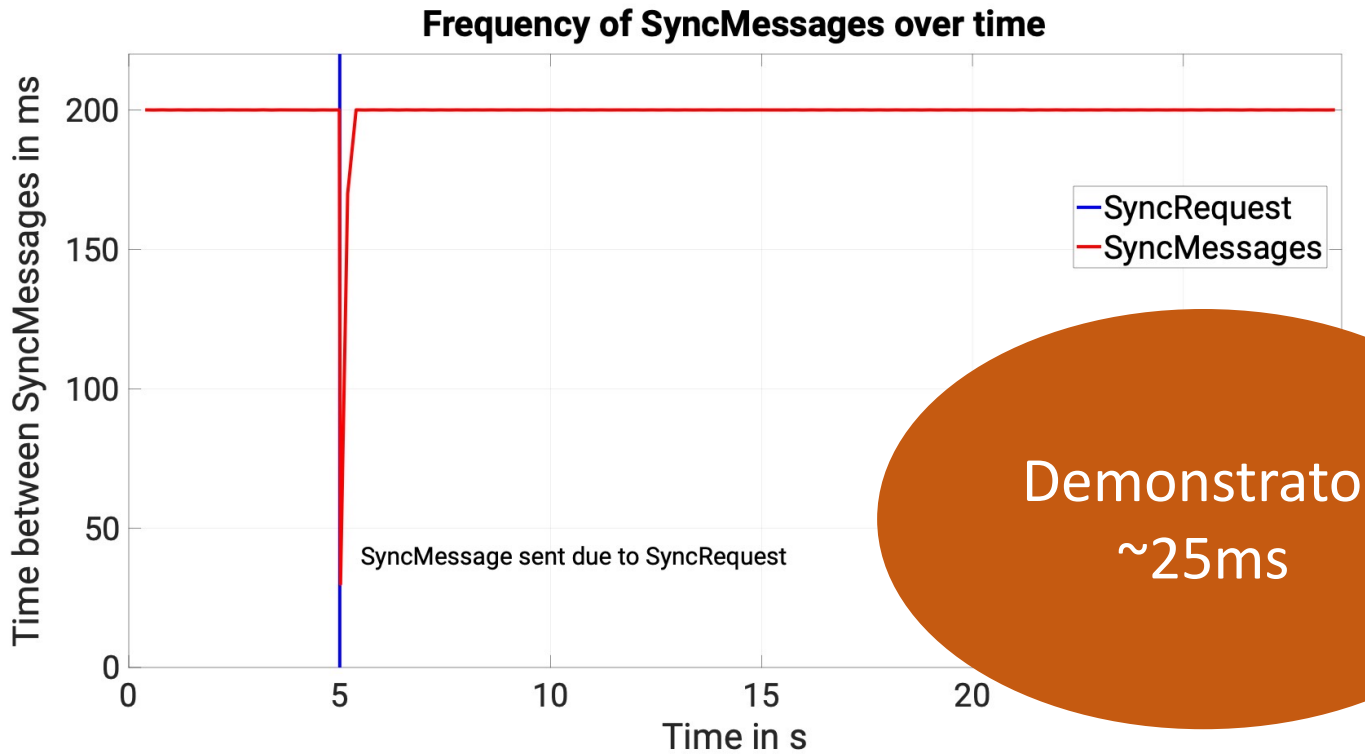
+ Synchronisation Request

[E] T. Rosenstatter and T. Olovsson, "*Extending AUTOSAR's Counter-based Solution for Freshness of Authenticated Messages in Vehicles*", PRDC 2019

Extension of AUTOSAR SecOC Profile 3

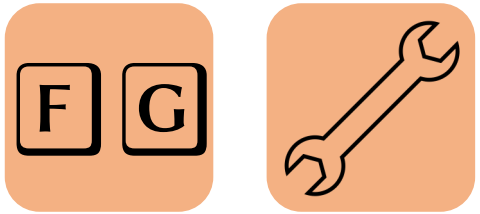
SyncRequest

+ additional security measures



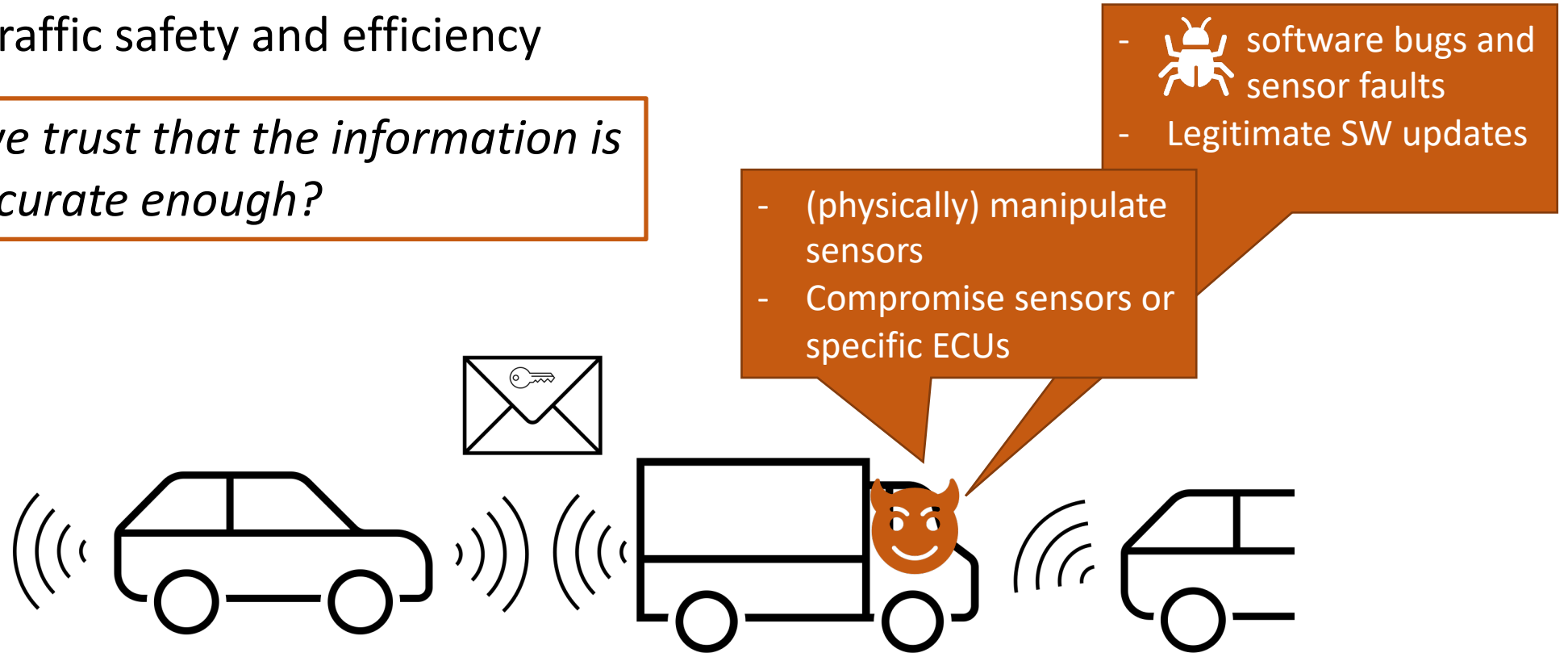
Demonstrator
~25ms

Cooperative Vehicles and Trust



- Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communication
- Increase traffic safety and efficiency

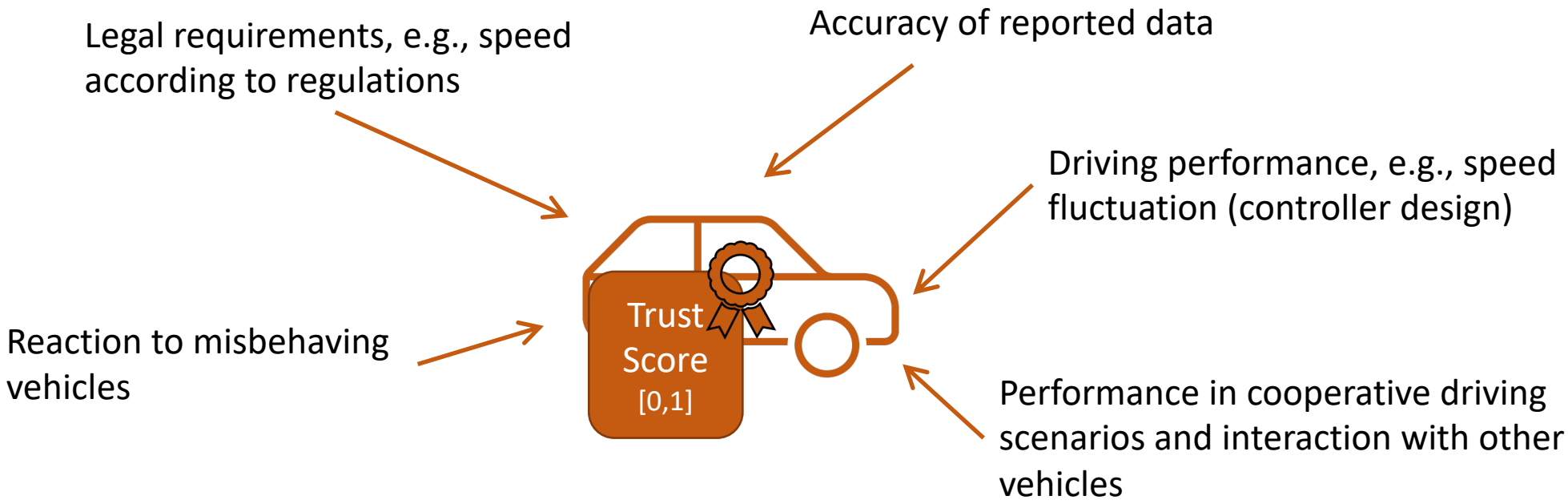
But how can we trust that the information is correct and accurate enough?



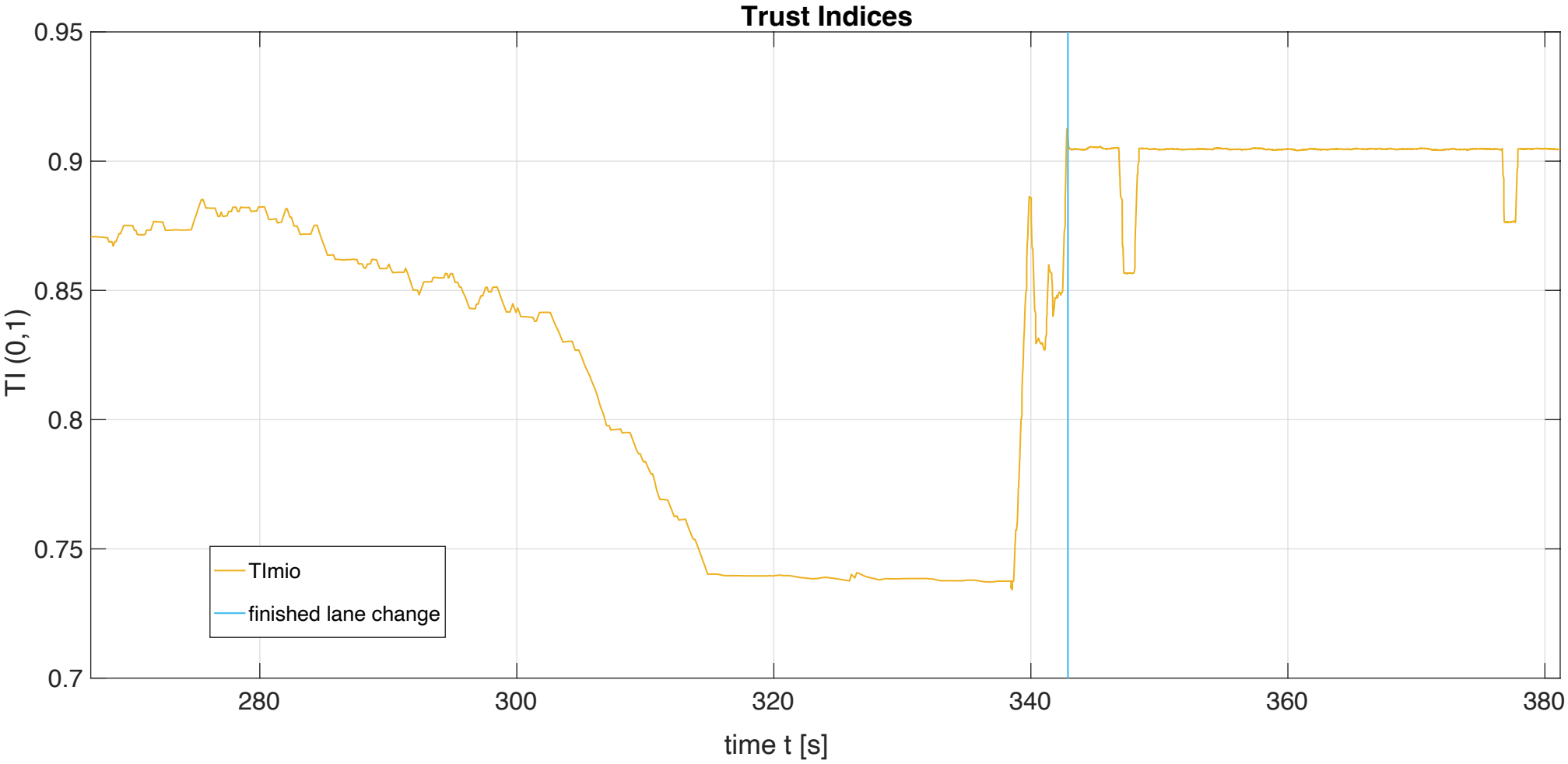
[F] M. Aramrattana et al., "*Team Halmstad Approach to Cooperative Driving in the Grand Cooperative Driving Challenge 2016*", T-ITS 2018
[G] T. Rosenstatter and C. Englund, "*Modelling the Level of Trust in a Cooperative Automated Vehicle Control System*", T-ITS 2018

A Trust Model for Cooperative Vehicles

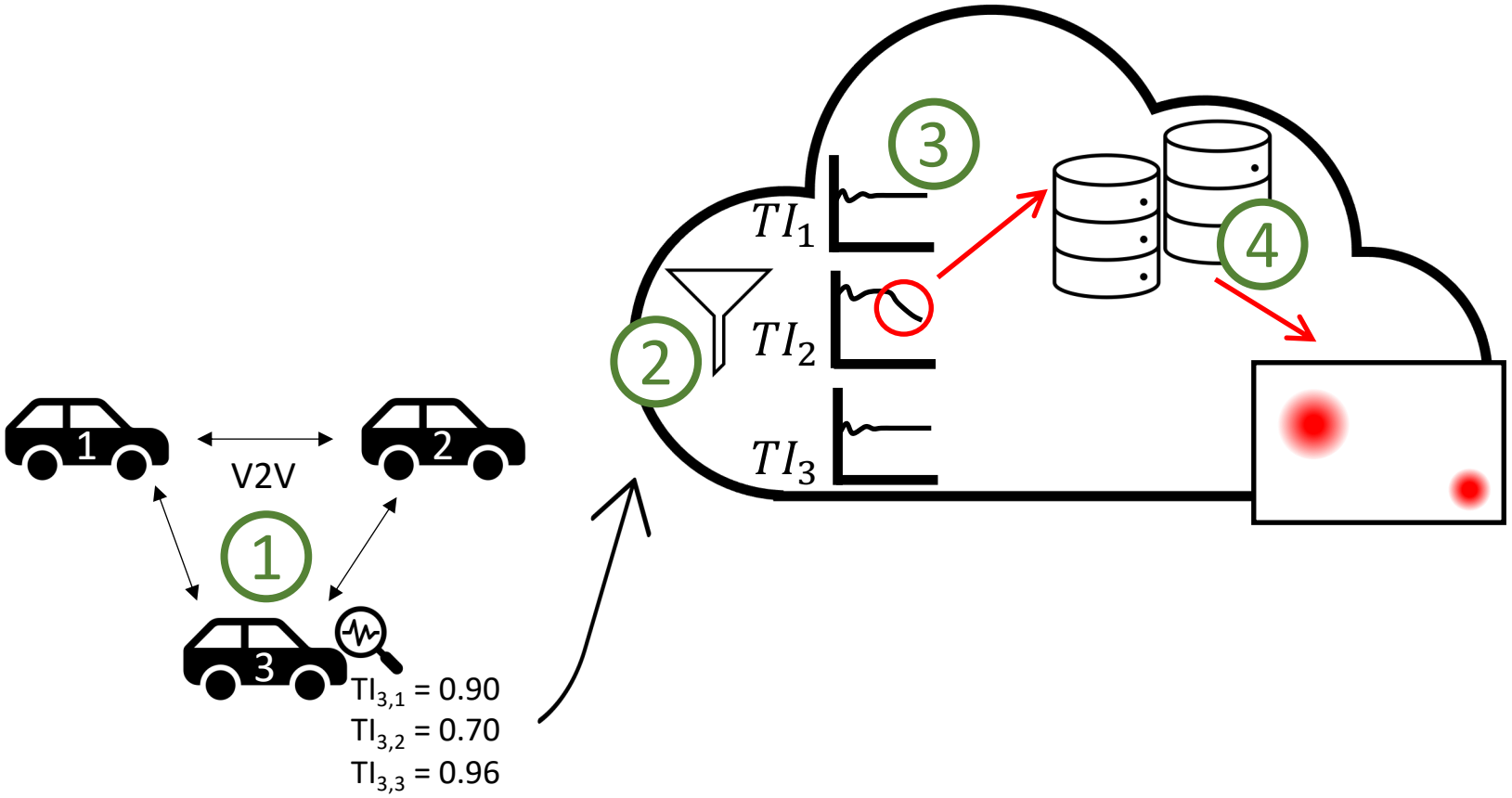
→Trust/Reputation model which computes a trust index (TI) or trust score considering the following factors:



A Trust Model for Cooperative Vehicles



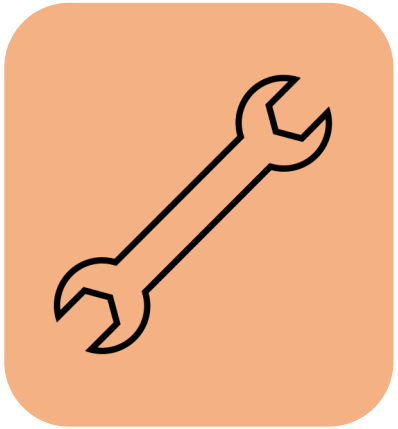
V2C Anomaly Detection



[H] T. Rosenstatter, T. Olovsson and M. Almgren, "*V2C A Trust-Based Vehicle to Cloud Anomaly Detection Framework for Automotive Systems*", ARES 2021

Part II. Generic Security Requirements and Identification of Suitable Techniques

- A B Linking security demands to generic security requirements
- C Taxonomy for resilience techniques
- D Resilience and security techniques based on analysing disclosed attacks



Part III. Design and Evaluation of Security and Resilience Techniques

- E Extension of a freshness mechanism
- F G A trust model for cooperative vehicles
- H Anomaly detection framework using Trust