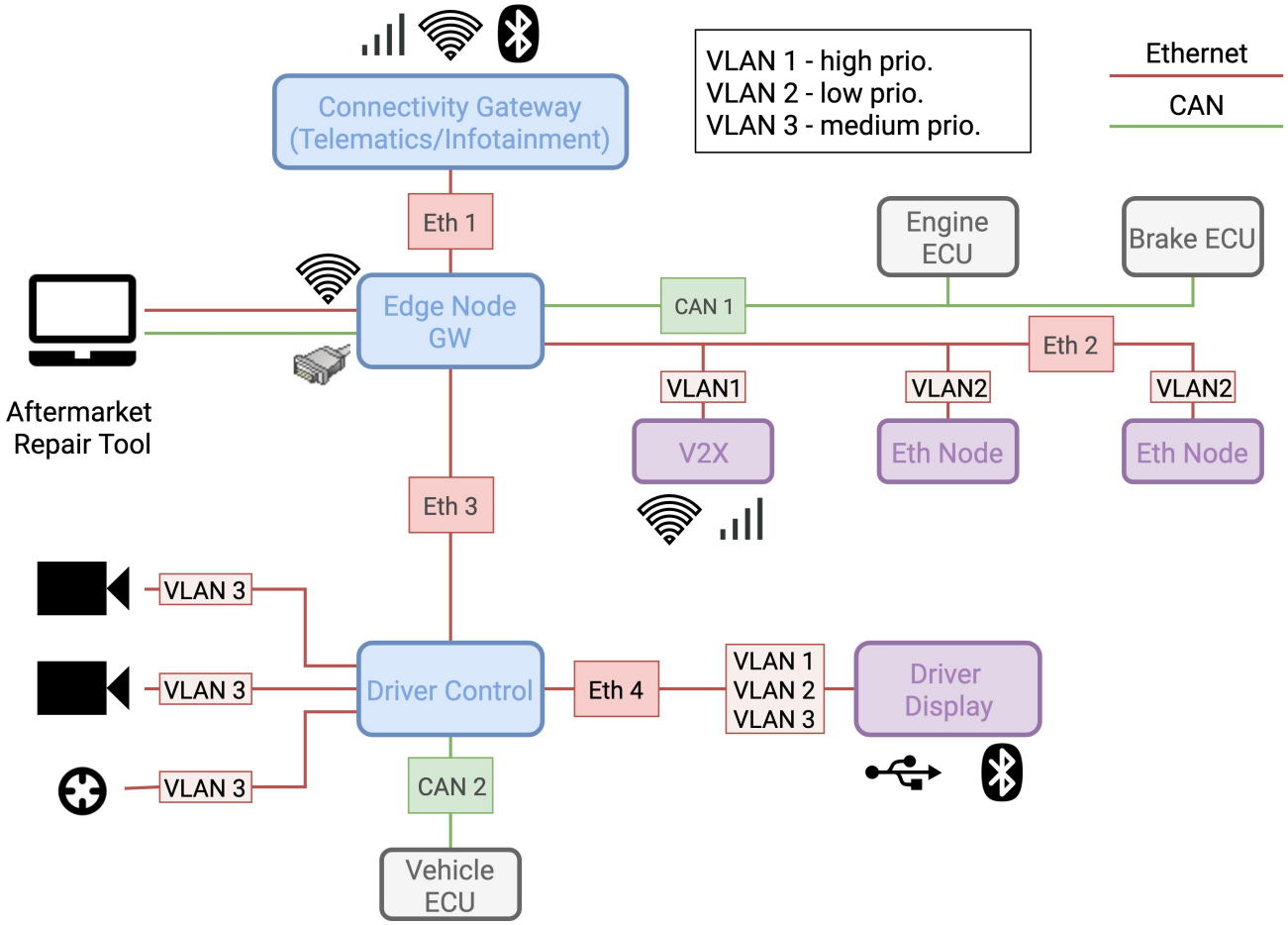
BRINGING AUTOMOTIVE SECURITY AND SAFETY CLOSER TOGETHER

17/12/2019

Thomas Rosenstatter

thomas.rosenstatter@chalmers.se

Simplified In-Vehicle Network

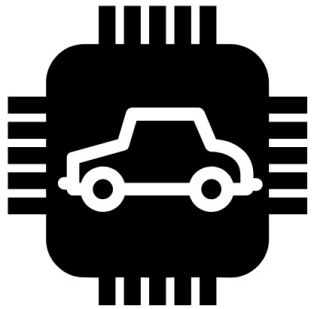


https://autosec.se/wp-content/uploads/2018/04/HOLISEC_D4.1.3_v1.0.pdf

Functional Safety

”absence of unreasonable risk due to hazards caused by malfunctioning behaviour of E/E systems” [ISO 26262]

Classifying **Safety** Demands



Hazard Analysis and Risk Assessment (HARA)

Hazardous Scenario	Severity	Exposure	Controllability
ABS fails	S[1-3]	E[1-4]	C[1-3]
...	...	...	...

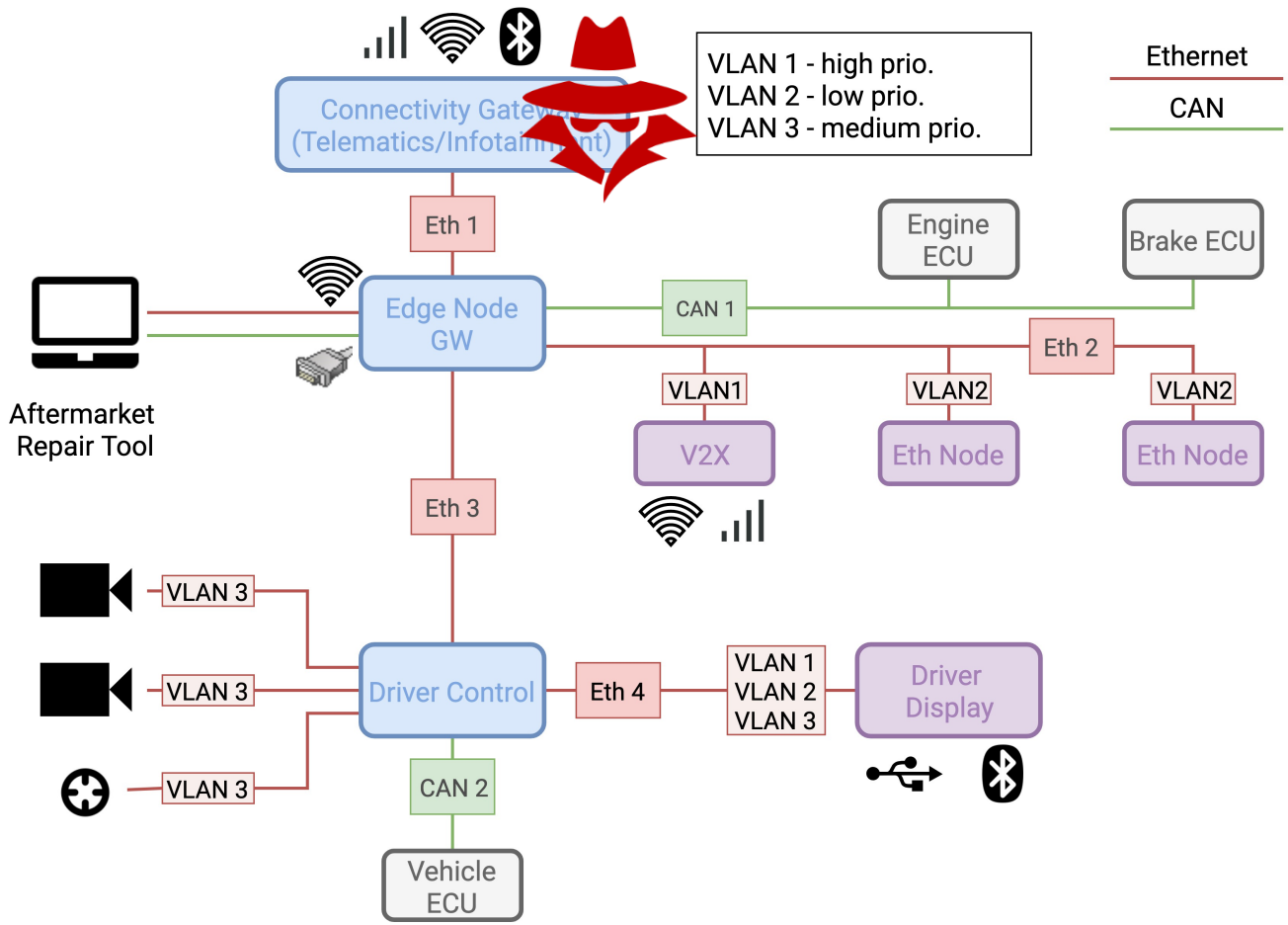
$$\begin{bmatrix} QM \\ A \\ B \\ C \\ D \end{bmatrix}$$

Safety Goal

Technical Safety Concept

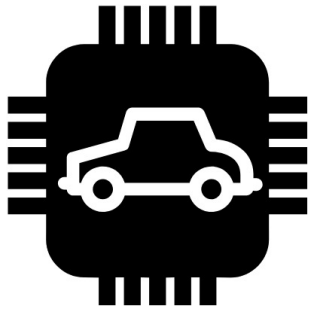
According to ISO 26262 – Functional Safety - Road Vehicles

Simplified In-Vehicle Network



https://autosec.se/wp-content/uploads/2018/04/HOLISEC_D4.1.3_v1.0.pdf

Classifying **Security** Demands



Threat Analysis and Risk Assessment (TARA)

Item	Threat	Knowledge	...
Speed	Spoofing	Standard	...
Speed	Tampering	Restricted	...
Break Signal	Tampering	Restricted	...
...	...	...	...

$$\begin{bmatrix} QM \\ 1 \\ 2 \\ 3 \\ 4 \end{bmatrix}$$

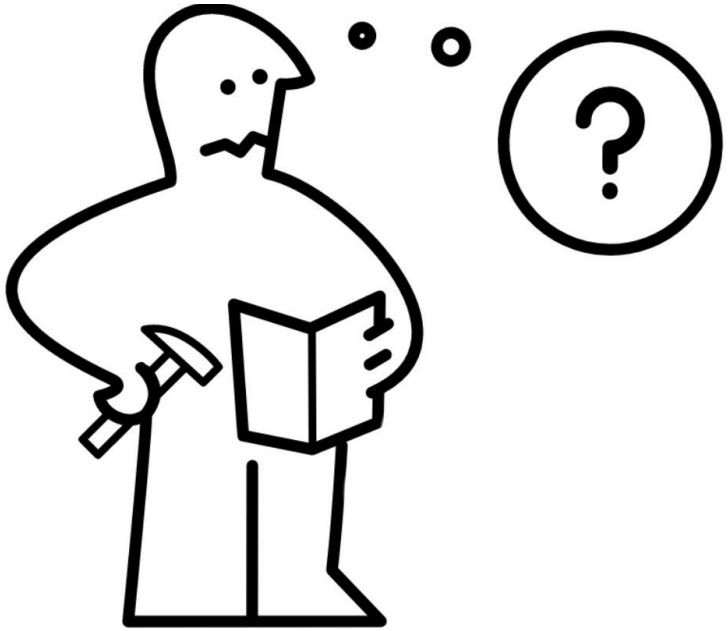
Cybersecurity Goals

Cybersecurity Requirements

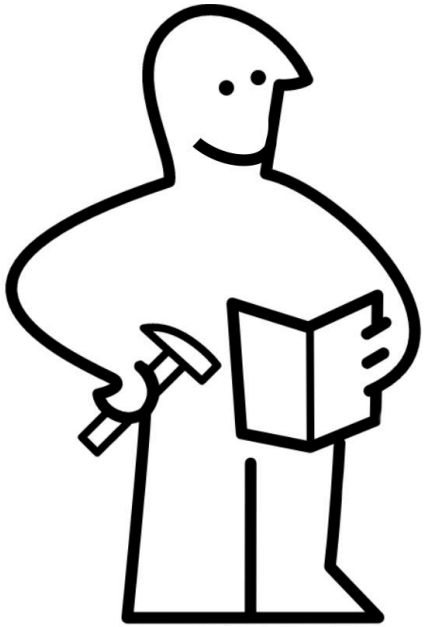
According to ISO 21434 -- Road Vehicles - Cybersecurity

Overview

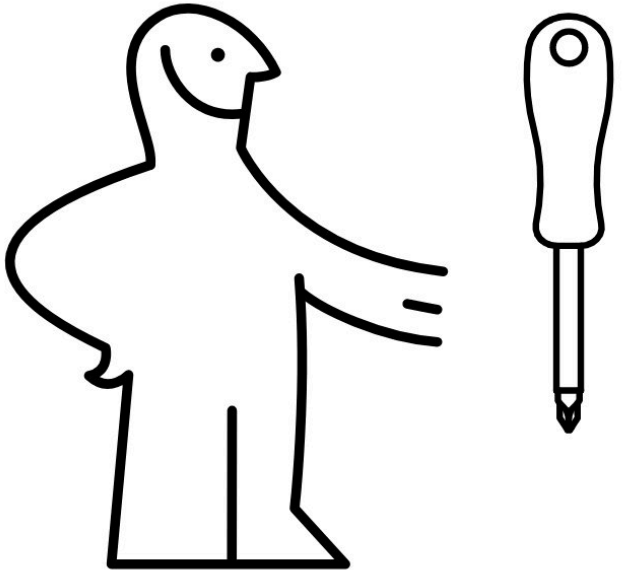
How?



What?

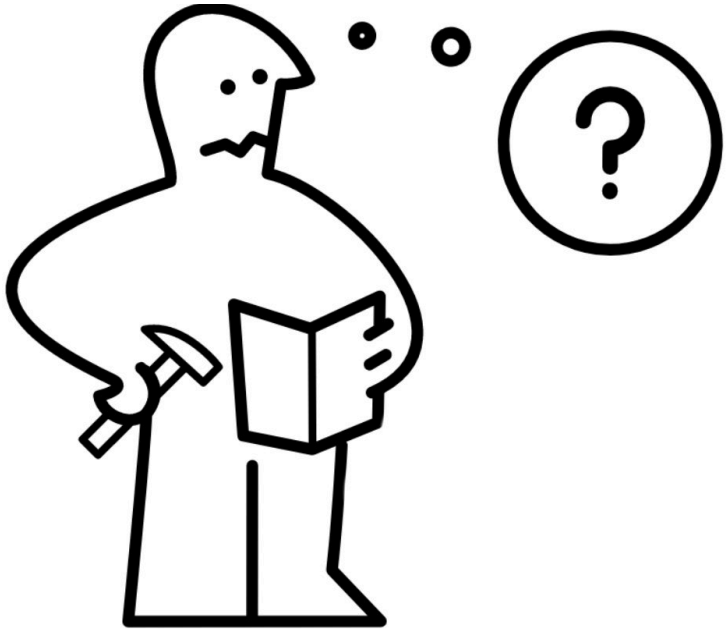


Safety and Security Requirements

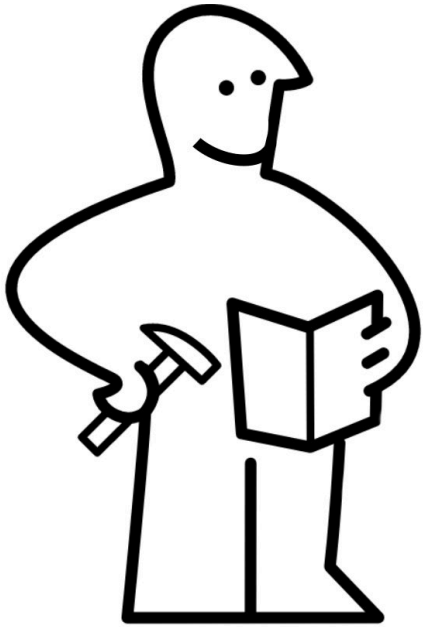


Overview

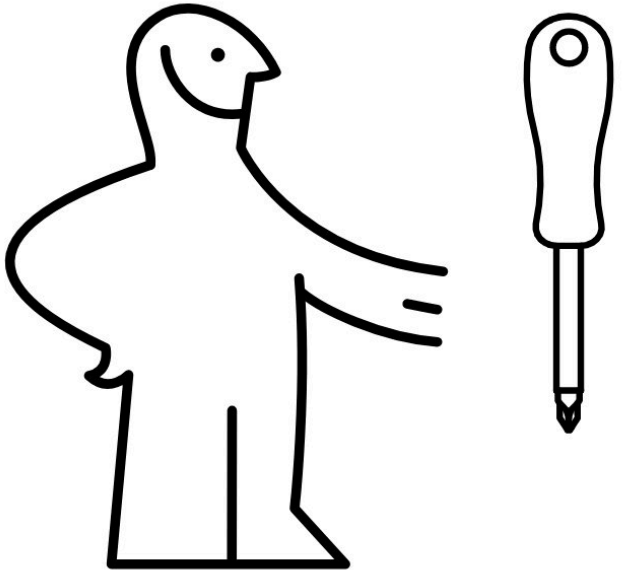
How?



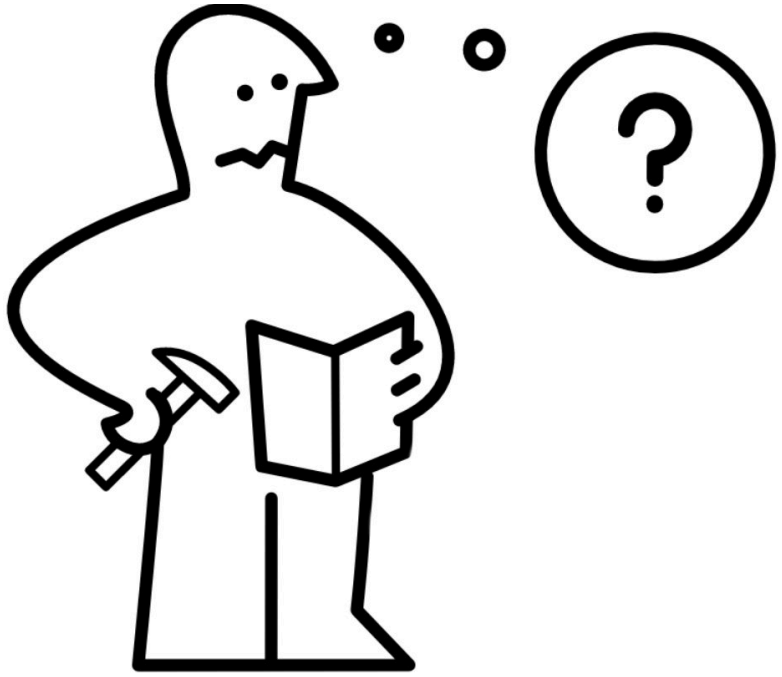
What?



Safety and Security Requirements



How?

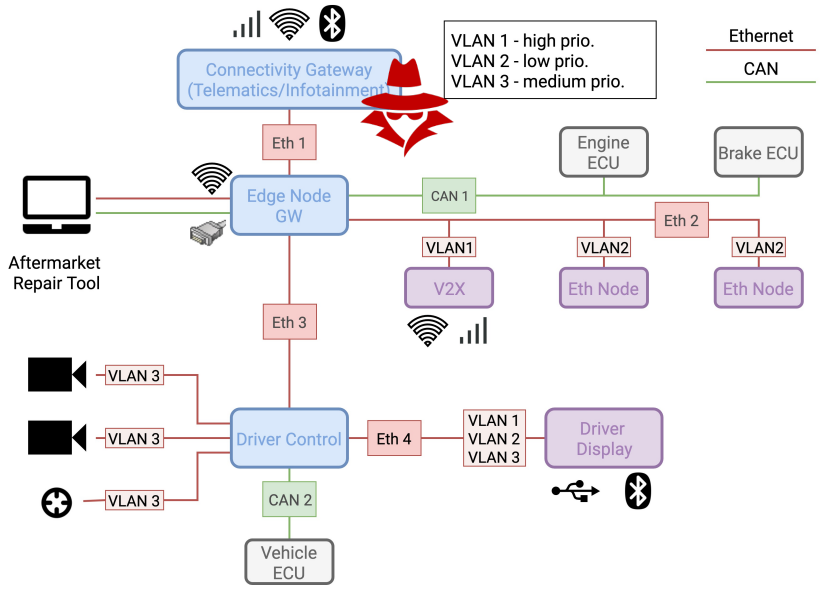


How should security demands be represented?

Rosenstatter, T. and Olovsson, T. (2018). **Open Problems when Mapping Automotive Security Levels to System Requirements**.In *Proceedings of the 4th International Conference on Vehicle Technology and Intelligent Transport Systems - Volume 1: VEHITS,* ISBN 978-989-758-293-6, pages 251-260. DOI: 10.5220/0006665302510260

Representation of Security Demands

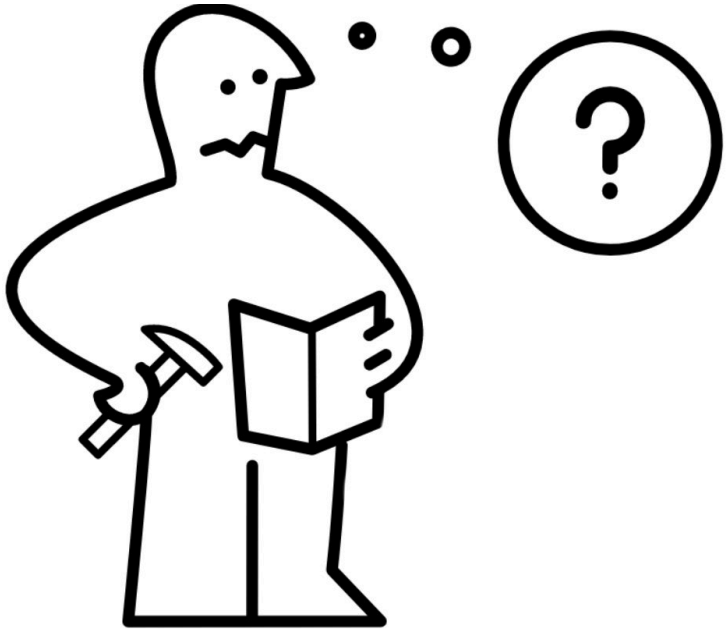
A vector is necessary



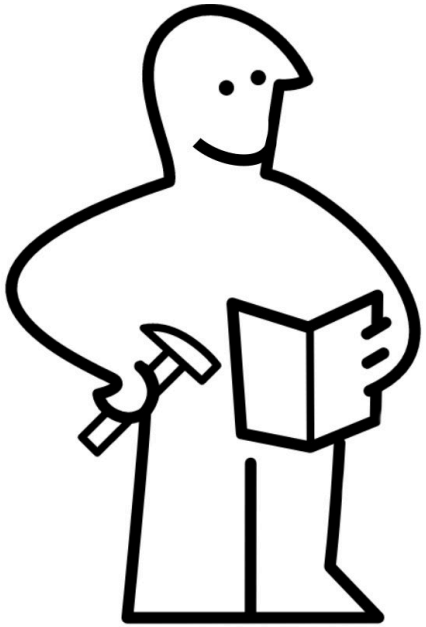
$$SL = \begin{bmatrix} Authenticity \\ Integrity \\ Non-Repudiation \\ Confidentiality \\ Availability \\ Authorisation \end{bmatrix} = \begin{bmatrix} 0 \dots 4 \\ 0 \dots 4 \\ 0 \dots 4 \\ 0 \dots 4 \\ 0 \dots 4 \\ 0 \dots 4 \end{bmatrix}$$

What?

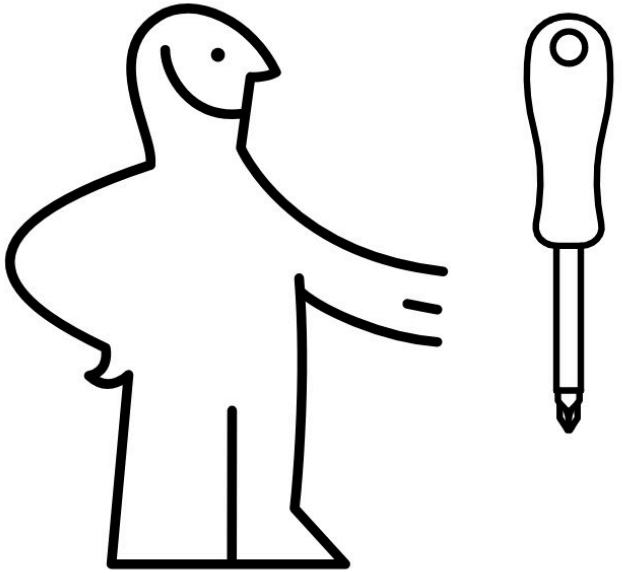
How?



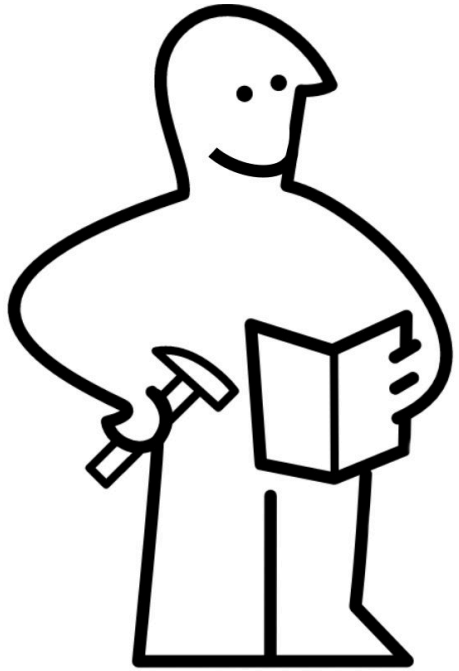
What?



Safety and Security Requirements



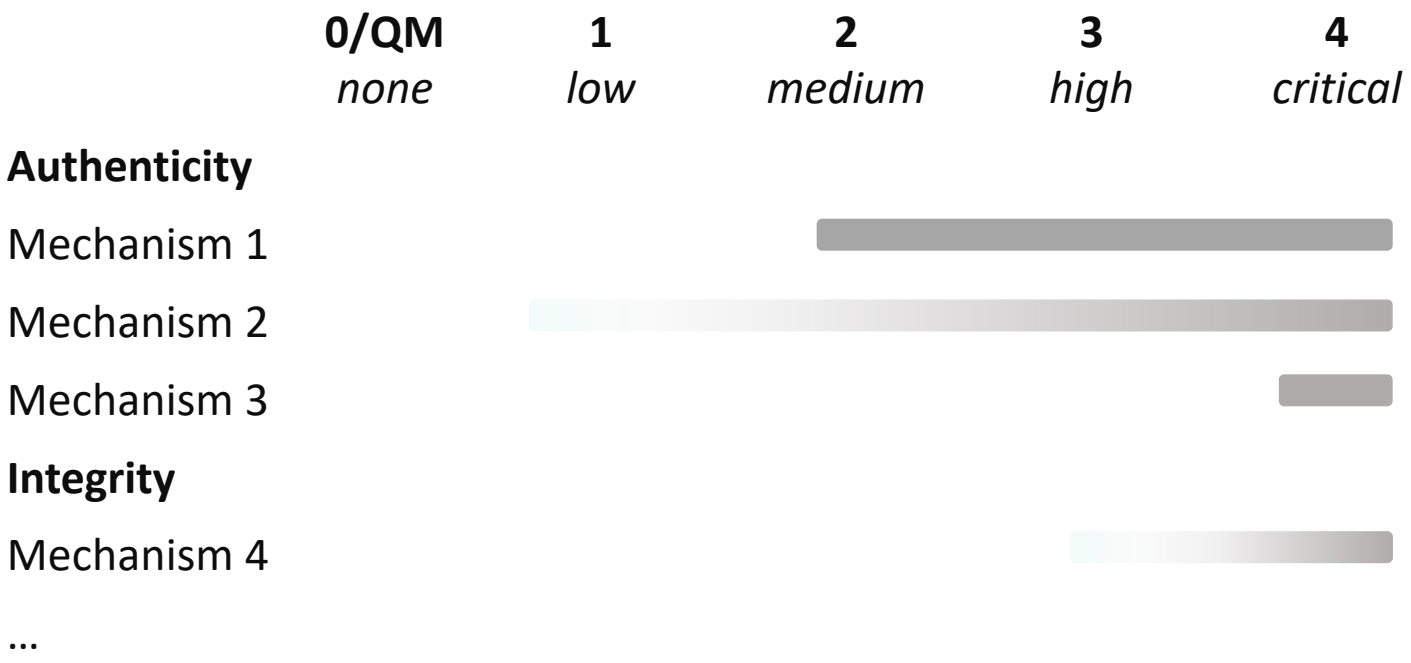
What?



What security mechanisms are necessary to be implemented?

T. Rosenstatter and T. Olovsson, **Towards a Standardized Mapping from Automotive Security Levels to Security Mechanisms** *2018 21st International Conference on Intelligent Transportation Systems (ITSC)*, Maui, HI, 2018, pp. 1501-1507.

Mapping to Security Mechanisms



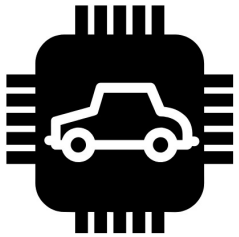
Identified mechanisms

		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					

Example: Authorisation

	SL 1	SL 2	SL 3	SL 4
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		1	1	2
AC.6 [MSG, FW, HW] Domain isolation			●	●

System Development Phase



Threat Analysis and Risk Assessment (TARA)

Item	Threat	Knowledge	...
Speed	Spoofing	Standard	...
Speed	Tampering	Restricted	...
Break Signal	Tampering	Restricted	...
...	...	...	...

$$\begin{bmatrix} 0 \dots 4 \\ 0 \dots 4 \\ 0 \dots 4 \\ 0 \dots 4 \\ 0 \dots 4 \\ 0 \dots 4 \end{bmatrix}$$

Cybersecurity Goals

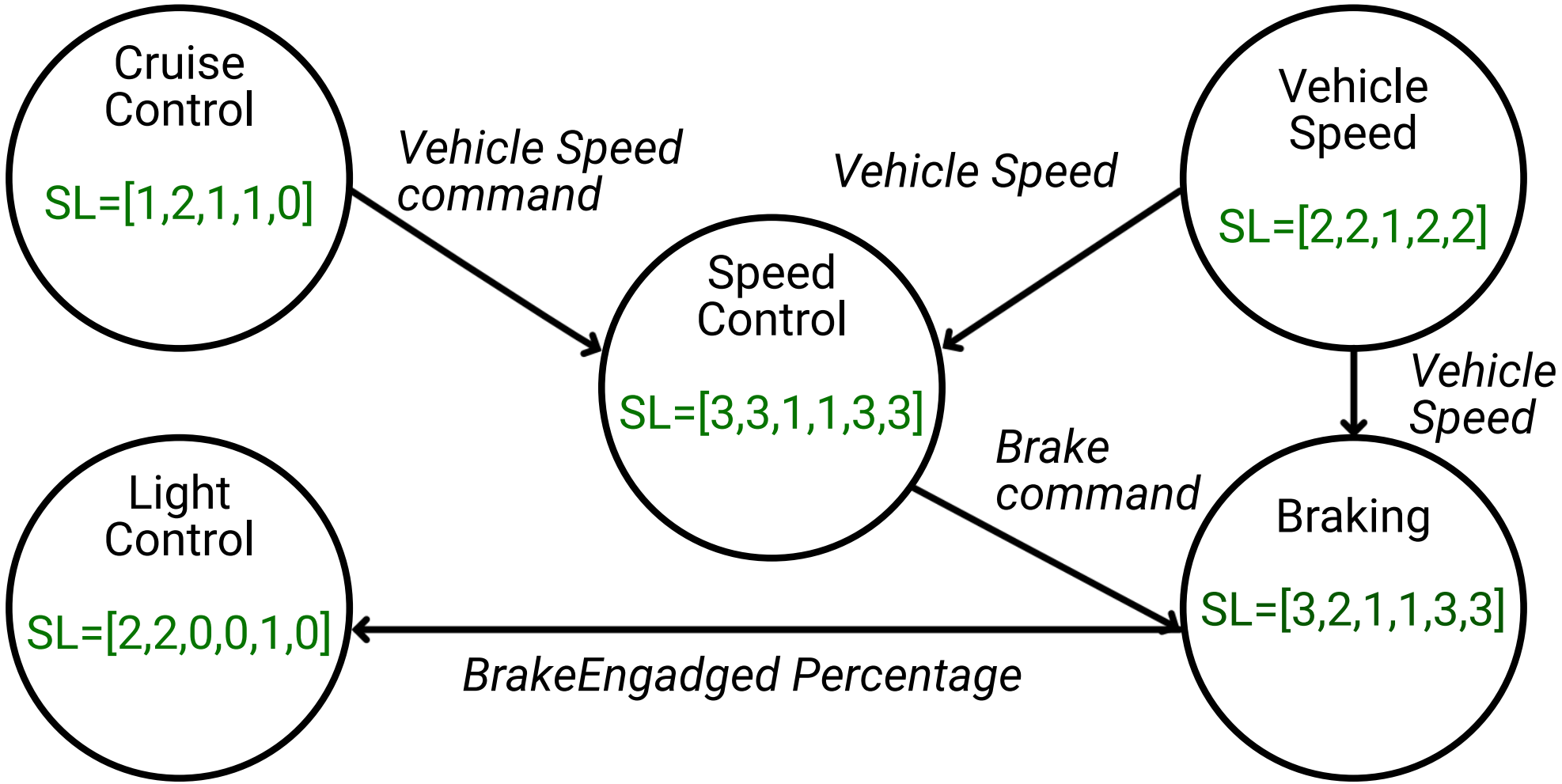
Selection of security mechanisms

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

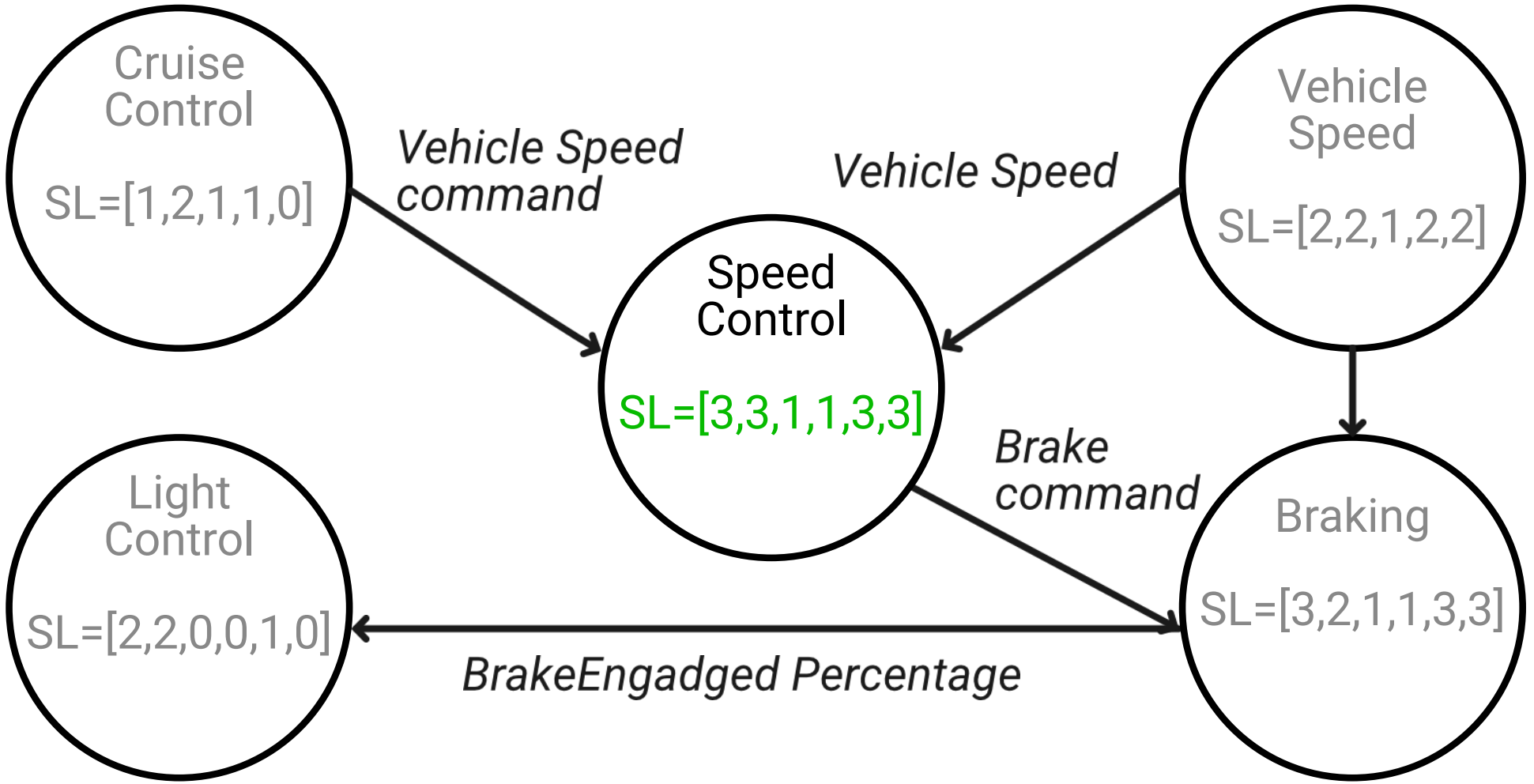
Cybersecurity Requirements

Adapted; ISO 21434 -- Road Vehicles – Cybersecurity

Use Case


Cruise Control
SL=[1,2,1,1,0]
Vehicle Speed command
Speed Control
SL=[3,3,1,1,3,3]
Vehicle Speed
Vehicle Speed
SL=[2,2,1,2,2]
Vehicle Speed
Brake command
Braking
SL=[3,2,1,1,3,3]
Light Control
SL=[2,2,0,0,1,0]
BrakeEngadged Percentage

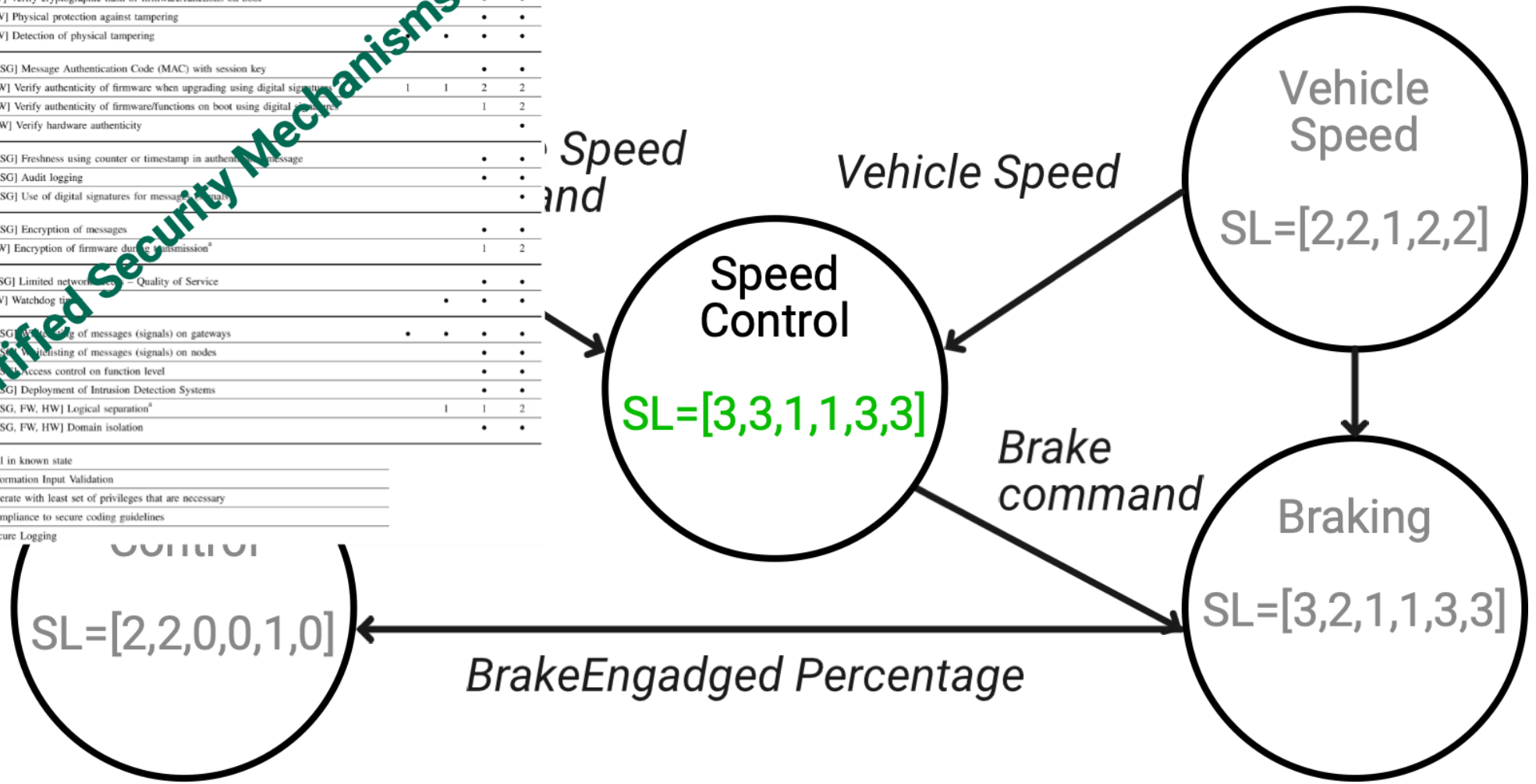
From Security Levels to Mechanisms



From Security Levels to Mechanisms

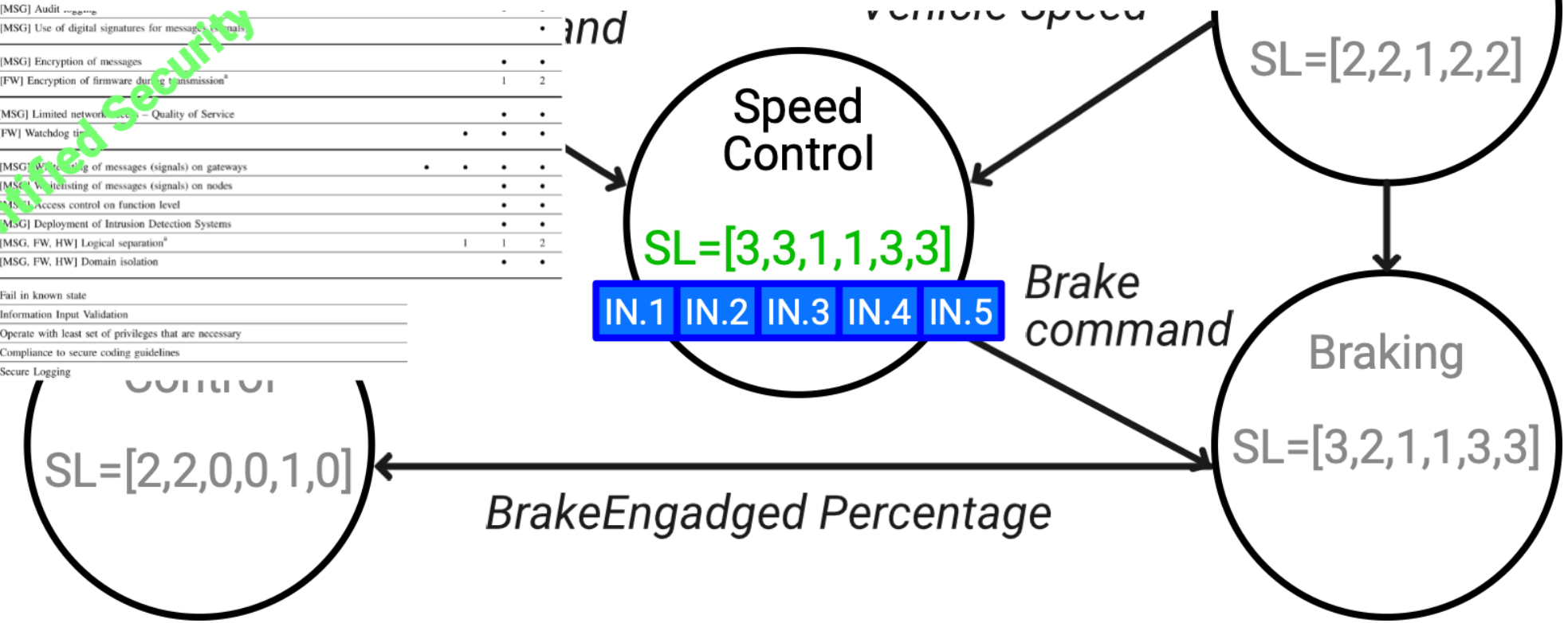
		SL 0	SL 1	SL 2	SL 3	SL 4
Integrity	IN.1 [MSG] Message Authentication Code (MAC) with pre-shared key			•	•	•
	IN.2 [FW] Verify cryptographic hash of firmware when upgrading		•	•	•	•
	IN.3 [FW] Verify cryptographic hash of firmware/functions on boot				•	•
	IN.4 [HW] Physical protection against tampering				•	•
	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 sig		1	1	2	2
	AU.3 [FW] Verify authenticity of firmware/functions on boot using digital				1	2
	AU.4 [HW] Verify hardware authenticity					•
Non-repudiation	NR.1 [MSG] Freshness using counter or timestamp in authen message				•	•
	NR.2 [MSG] Audit logging				•	•
	NR.3 [MSG] Use of digital signatures for messa					•
Confidentiality	CO.1 [MSG] Encryption of messages				•	•
	CO.2 [FW] Encryption of firmware dur transmission[a]				1	2
Availability	AV.1 [MSG] Limited netwo – Quality of Service				•	•
	AV.2 [FW] Watchdog ti			•	•	•
Authorization and Access Control	AC.1 [MSG] g of messages (signals) on gateways		•	•	•	•
	AC.2 [MS ltering of messages (signals) on nodes				•	•
	AC.3 [M Access control on function level				•	•
	[MSG] Deployment of Intrusion Detection Systems				•	•
	[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					

Identified Security Mechanisms

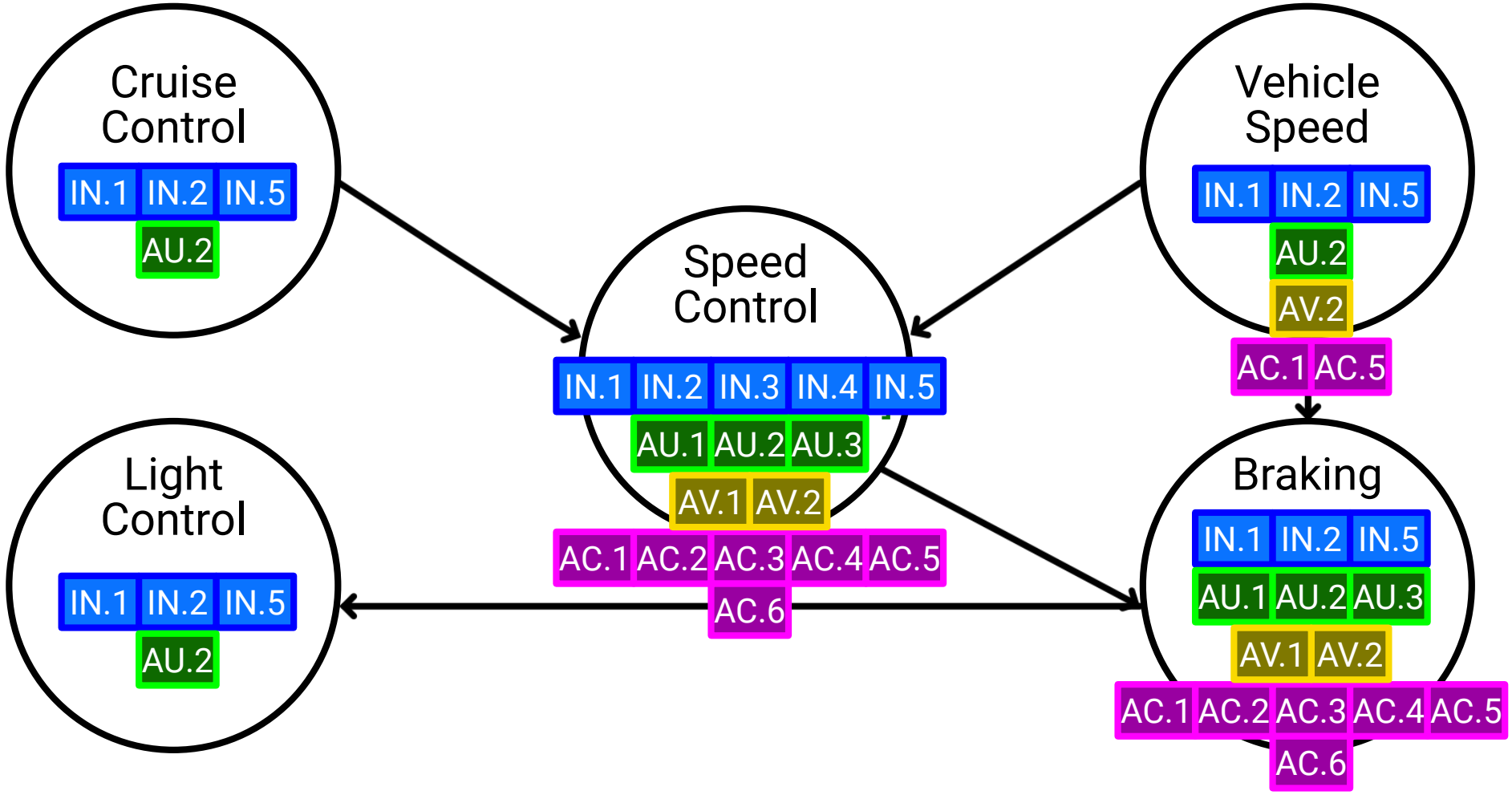


From Security Levels to Mechanisms

		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		•	•	•	•

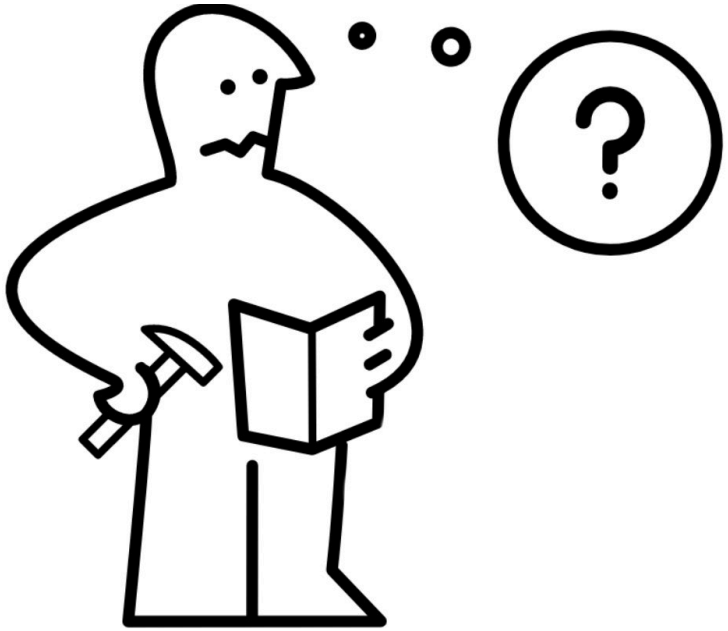


From Security Levels to Mechanisms

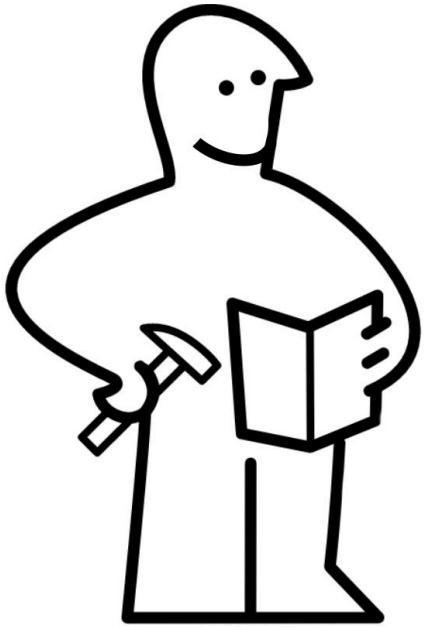


Safety and Security

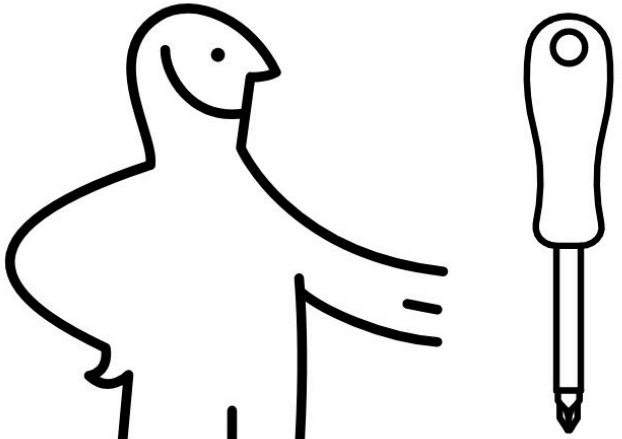
How?



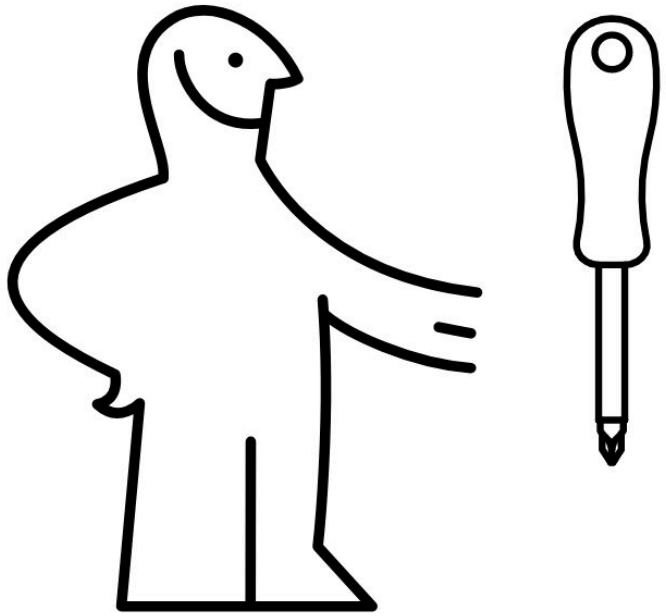
What?



Safety and Security Requirements



Safety and Security



Bringing safety and security closer together

Safety and Security



Hazard Analysis and Risk Assessment (HARA)

Hazardous Scenario	Severity	Exposure	Controllability
ABS fails	S[1-3]	E[1-4]	C[1-3]
...	...	...	...

$$\begin{bmatrix} QM \\ A \\ B \\ C \\ D \end{bmatrix}$$

Safety Goal → **Technical Safety Concept**

- Well established
- (clear) requirements/recommendations e.g., Independent parallel redundancy can be realised as dissimilar software in each parallel path.

- More complex
- Mapping to mechanisms covers basic security needs
- Interplay between safety and security <u>needs</u> to be addressed

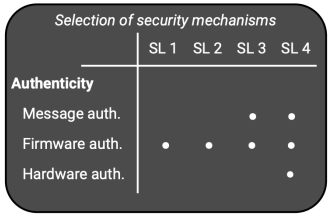


Threat Analysis and Risk Assessment (TARA)

Item	Threat	Knowledge	...
Speed	Spoofing	Standard	...
Speed	Tampering	Restricted	...
Break Signal	Tampering	Restricted	...
...	...	...	...

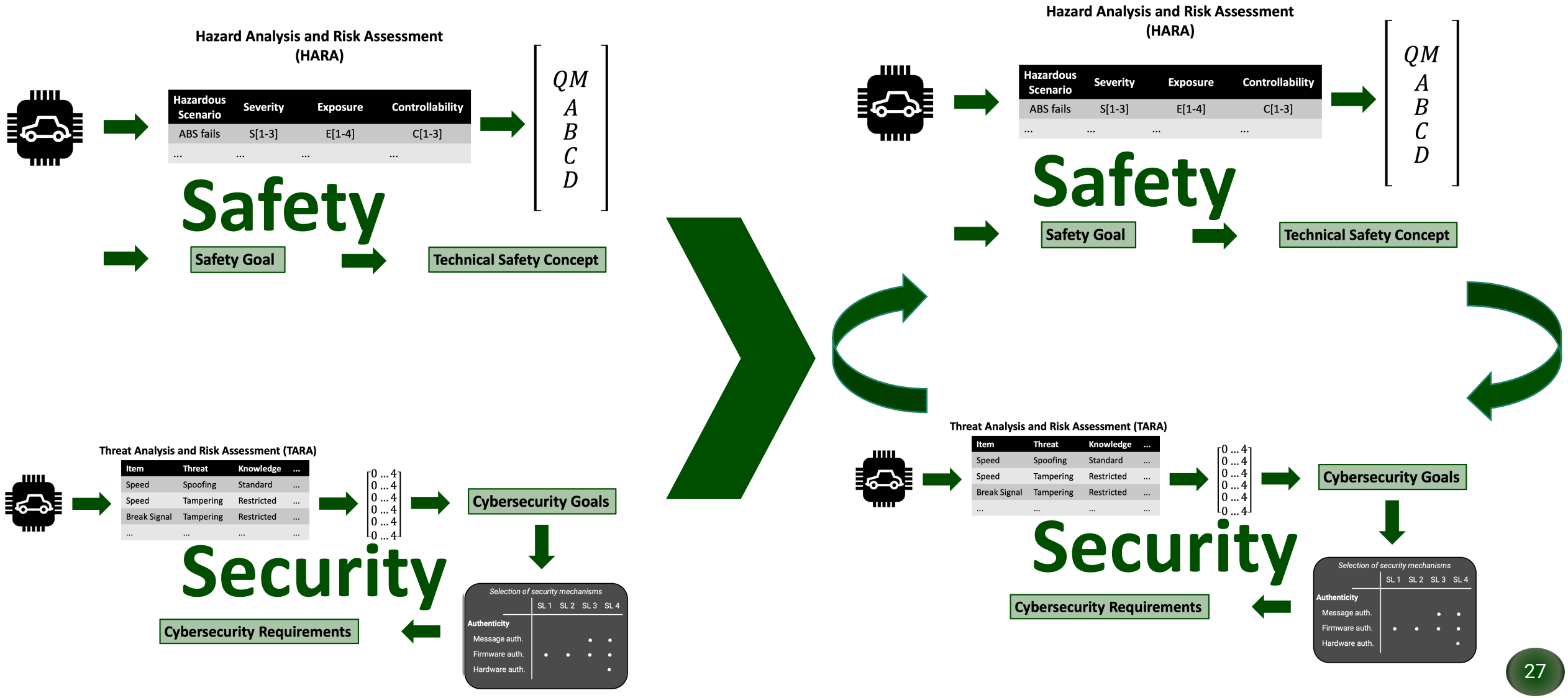
$$\begin{bmatrix} 0 \dots 4 \\ 0 \dots 4 \\ 0 \dots 4 \\ 0 \dots 4 \\ 0 \dots 4 \\ 0 \dots 4 \end{bmatrix}$$

Cybersecurity Goals



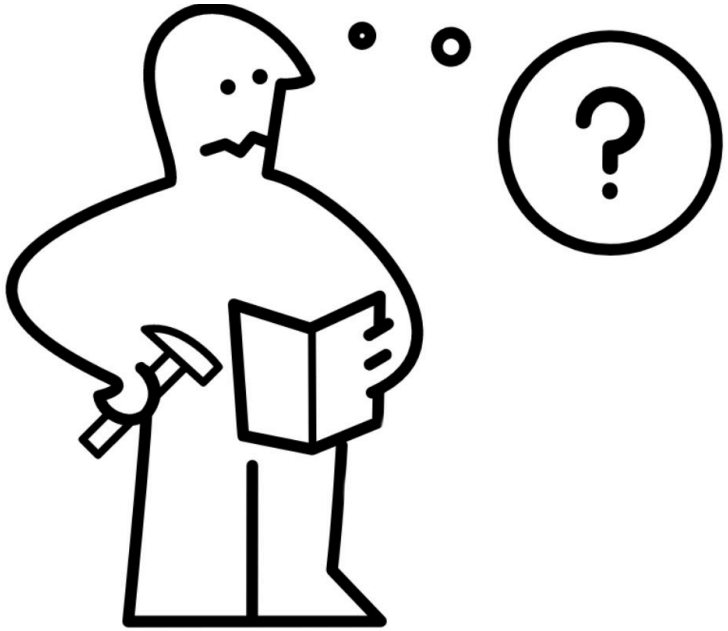
Cybersecurity Requirements

Safety and Security

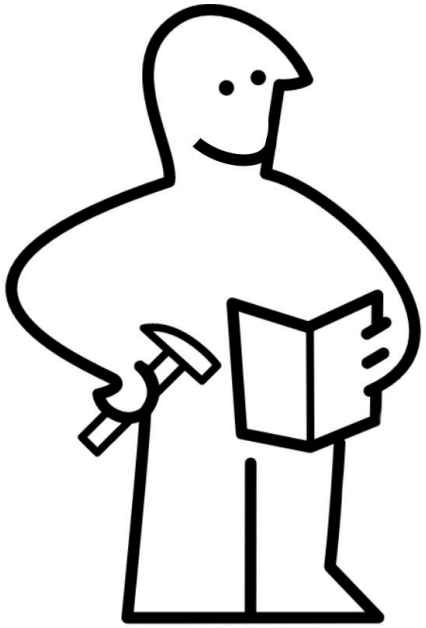


BRINGING AUTOMOTIVE SECURITY AND SAFETY CLOSER TOGETHER

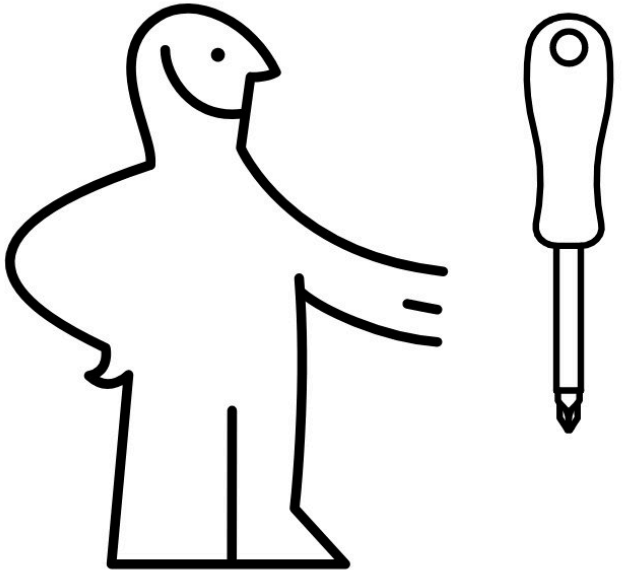
How?



What?



Safety and Security Requirements



Illustrations in overview slides modified from ikea.se assembly manuals