

AUtomotive Risk Assessment

Study and application of the MAGERIT methodology and the PILAR tool to an automotive scenario

AURA

rev³rse
SECURITY

Mario Raciti

Who Am I

Mario Raciti

- Cybersecurity Enthusiast
- Writer @rev3rsesecurity

My Contacts

tsumarios.github.io

 marioraciti@pm.me

 marioraciti

 tsumarios

 tsumarios

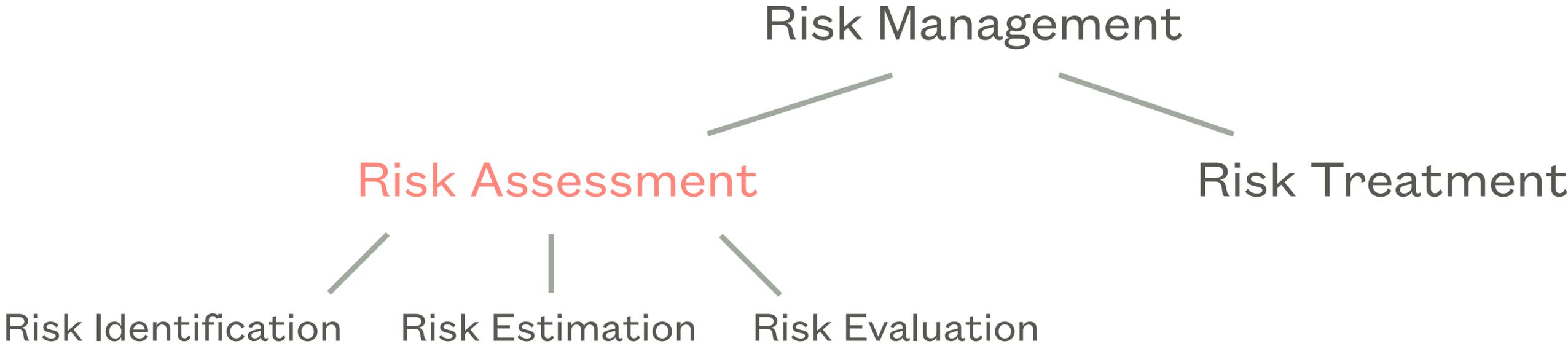
Risk Management

“If you don't invest in risk management,
it doesn't matter what business you're in, it's a risky business.”

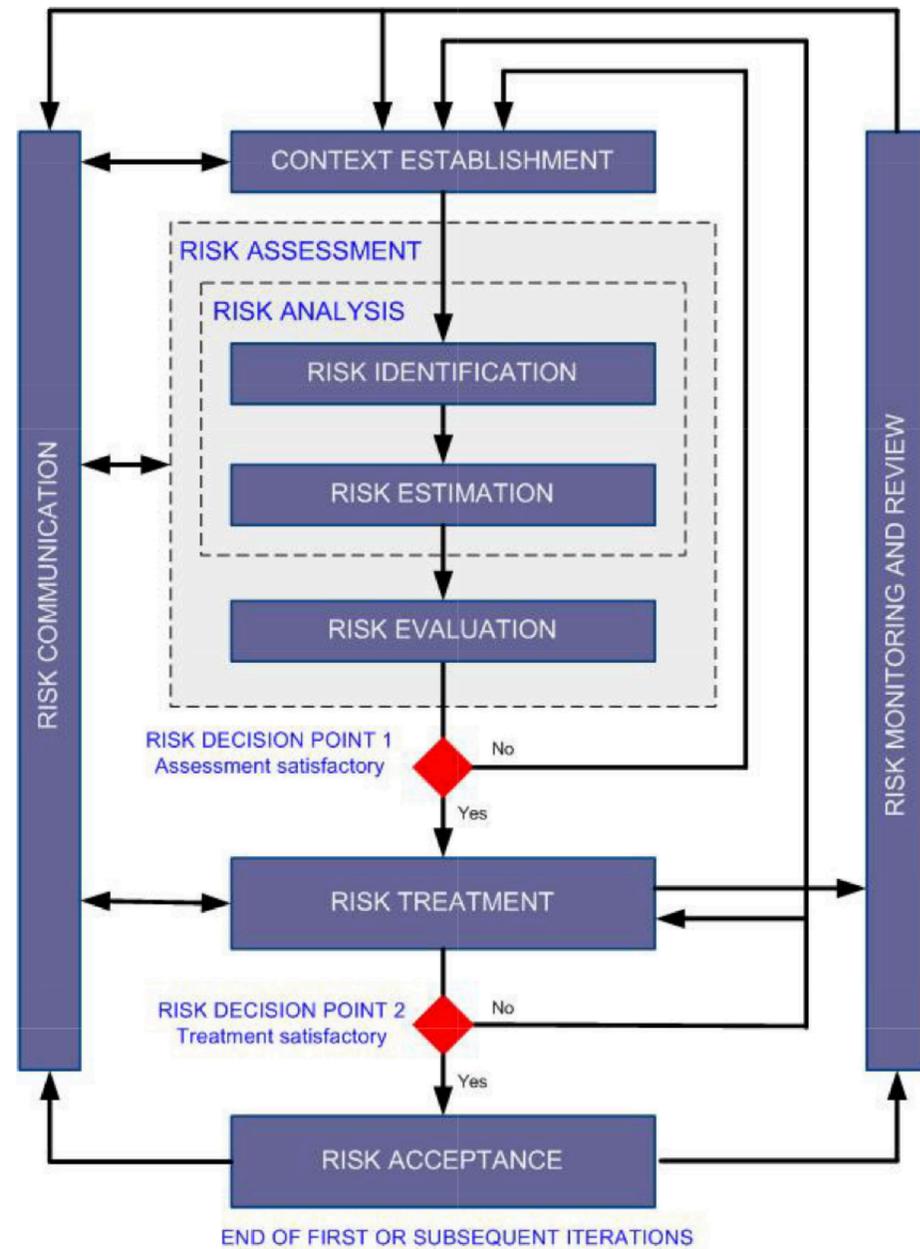
Gary Cohn



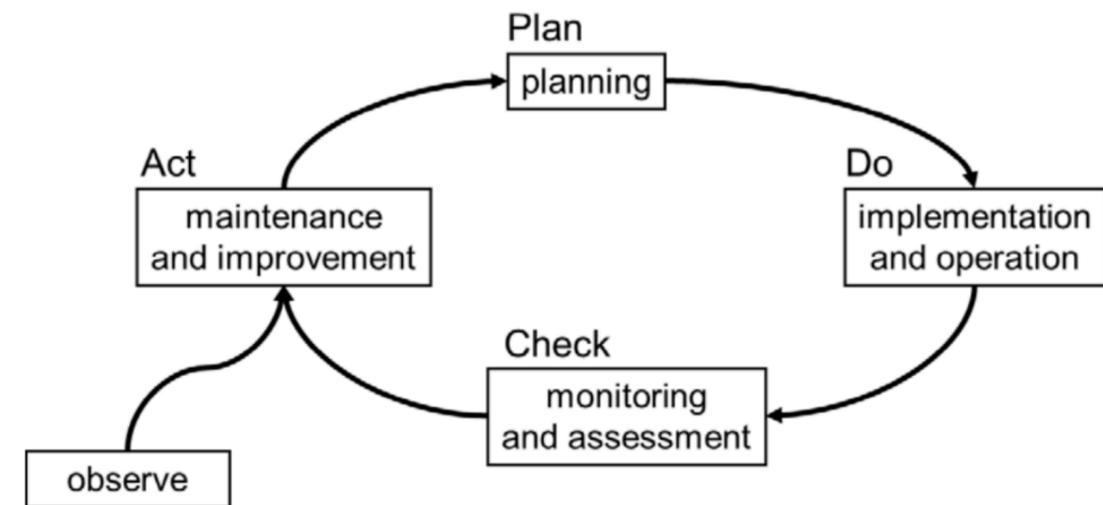
RM in a Nutshell



RM Topology



ISO 27005



ISMS PDCA Cycle [ISO 27001]

MAGERIT

Magerit responds to what is called:
“Risk Management Process” [ISO 31000]



- Developed by the Spanish Ministry of Public Administrations
- Framework and guide to the Public Administration (and more for its open nature)
- Compliance: ISO 31000:2009, ISO 27001:2005, ISO 15408:2005, ISO 17799:2005, ISO 13335:2004

Five phases: **Risk identification** -> **Threats** -> **Safeguards** -> **Risk analysis** -> **Risk evaluation**

PILAR

Pilar is a tool that supports Magerit

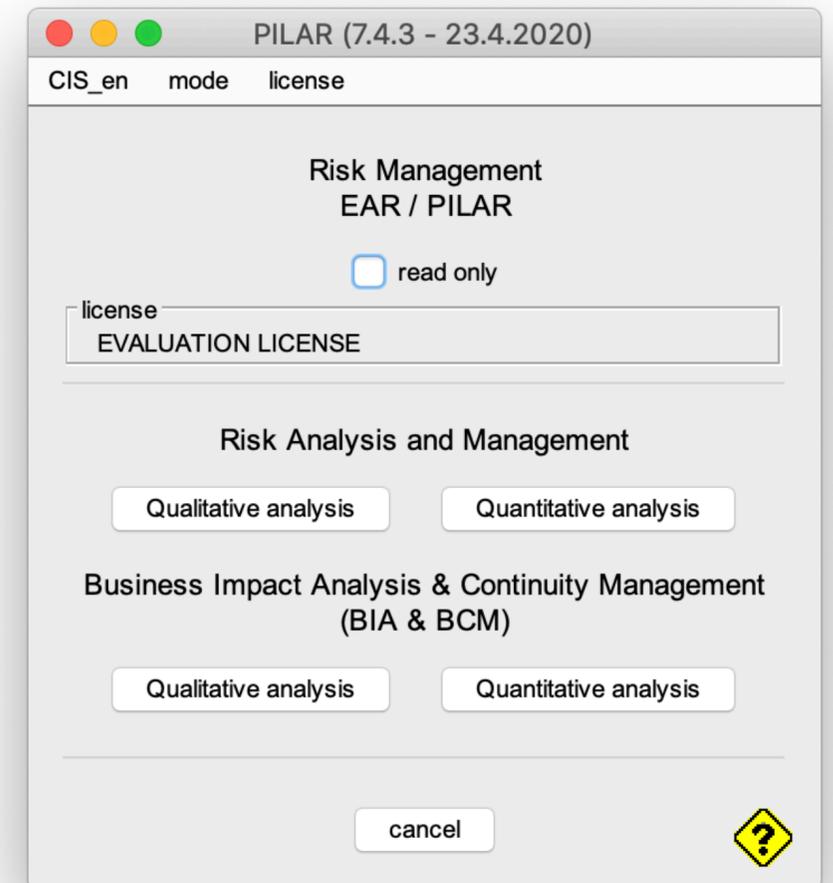
- Partly funded by the Centro Criptológico Nacional (NSA)
- Provides a standard library for assets, threats and safeguards
- ISO 27002:2005 - Code of practice for information security management
- General Data Protection Regulation (GDPR) 2016/679

Qualitative analysis may be used:

- as an initial assessment to identify risks
- where there is a lack of info or resources

Quantitative analysis depends on:

- the accuracy of the assigned values
- the validity of the statistical models used



RA Concepts

RA inputs:

- Assets
- Threats
- Safeguards

Other factors:

- Security dimensions
- Likelihood

RA outputs:

- Impact
- Risk

<i>Risk</i>		<i>Likelihood</i>				
		VL	L	M	H	VH
<i>Impact</i>	VH	H	VH	VH	VH	VH
	H	M	H	H	VH	VH
	M	L	M	M	H	H
	L	VL	L	L	M	M
	VL	VL	VL	VL	L	L

Risk for dummies $R = L \times I$

Actual risk $R = \dots?$

where R is the risk, L the likelihood and I the impact.

PILAR Reverse Engineering

Impact $I = V \times d$

where I is the impact, V the asset value and d the degradation.

PILAR Impact $I = V - \delta$ where $\delta = \begin{cases} 6 & \text{if } d = 1 \% \\ 3 & \text{if } d = 10 \% \\ 2 & \text{if } d = 20 \% \\ 1 & \text{if } d = 50 \% \\ 0 & \text{if } d = 100 \% \end{cases}$

Exponential fit $y = 1002.75e^{0.767241x}$ with $r = 0.99$

E.g. $V = 6$ (= 100000), $d = 20 \%$

$$I = V - \delta = 6 - 2 = 4$$

$$I = V \times d = 100000 \times 20 \% = 20000 \simeq_{(Exp\ fit)} 3.9 \simeq 4$$

Level	Value
0	1000
1	2150
2	4650
3	10000
4	21500
5	46500
6	100000
7	215000
8	465000
9	1000000
10	2150000

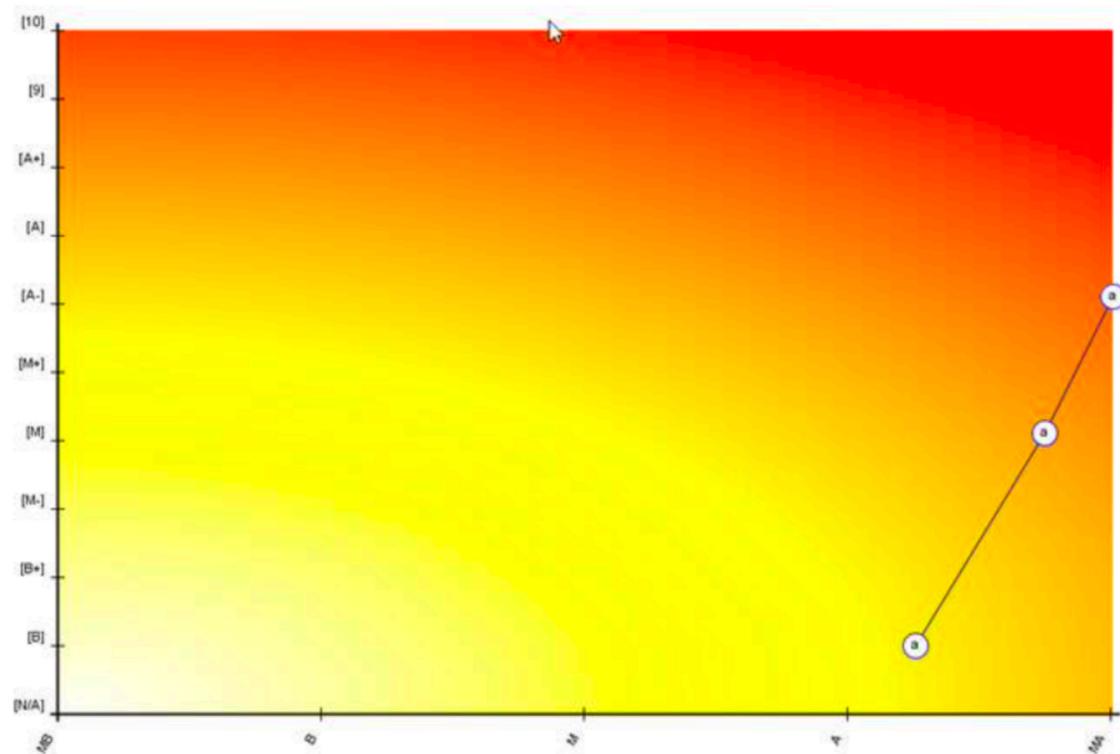
PILAR Levels Map

PILAR Reverse Engineering

PILAR Conjectured Risk

$$R = 0.6I + \lambda$$

where R is the risk, I the impact and $\lambda = \begin{cases} -0.9 & \text{if } L = VL \\ 0 & \text{if } L = L \\ 0.9 & \text{if } L = M \\ 1.8 & \text{if } L = H \\ 2.7 & \text{if } L = VH \end{cases}$



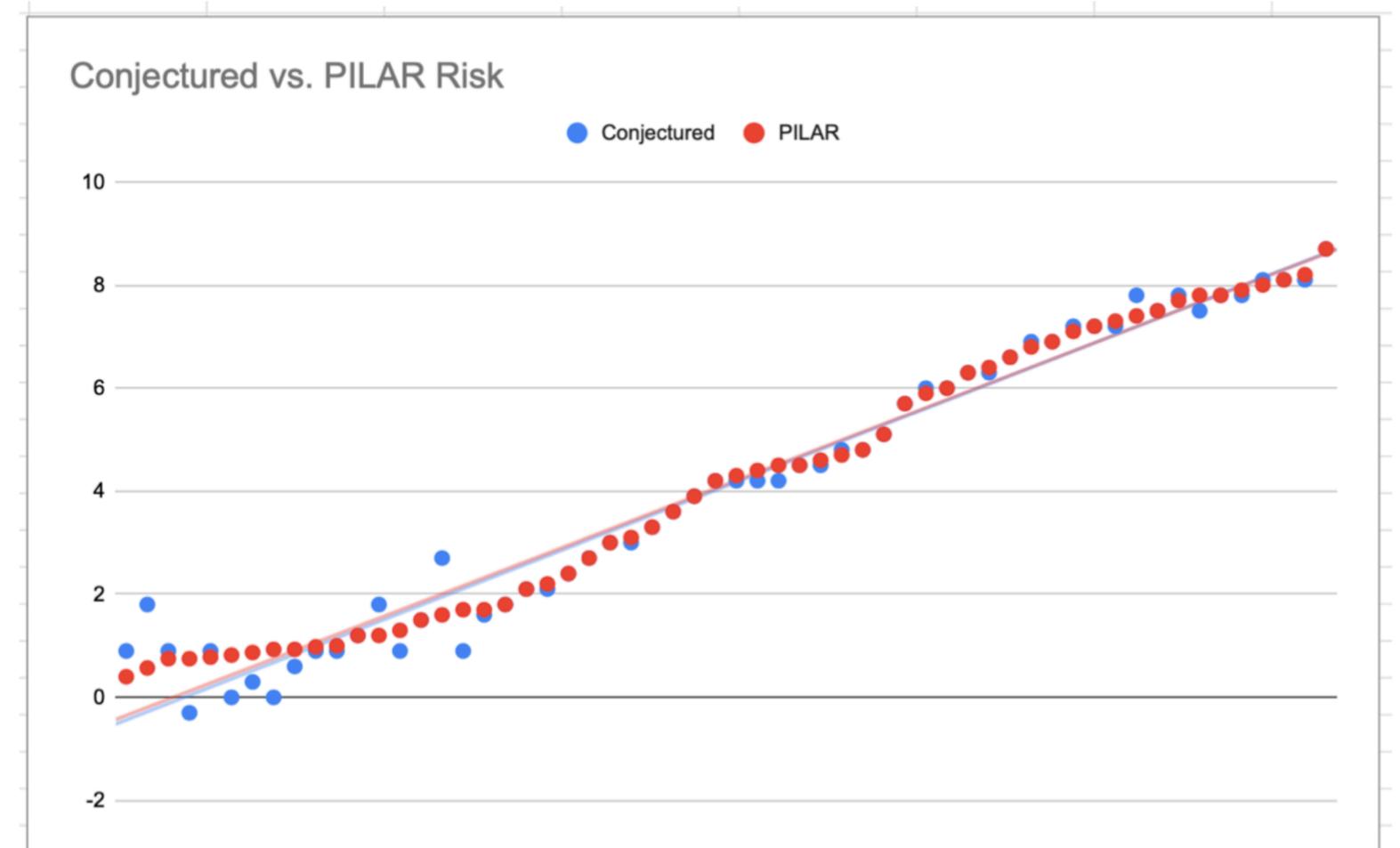
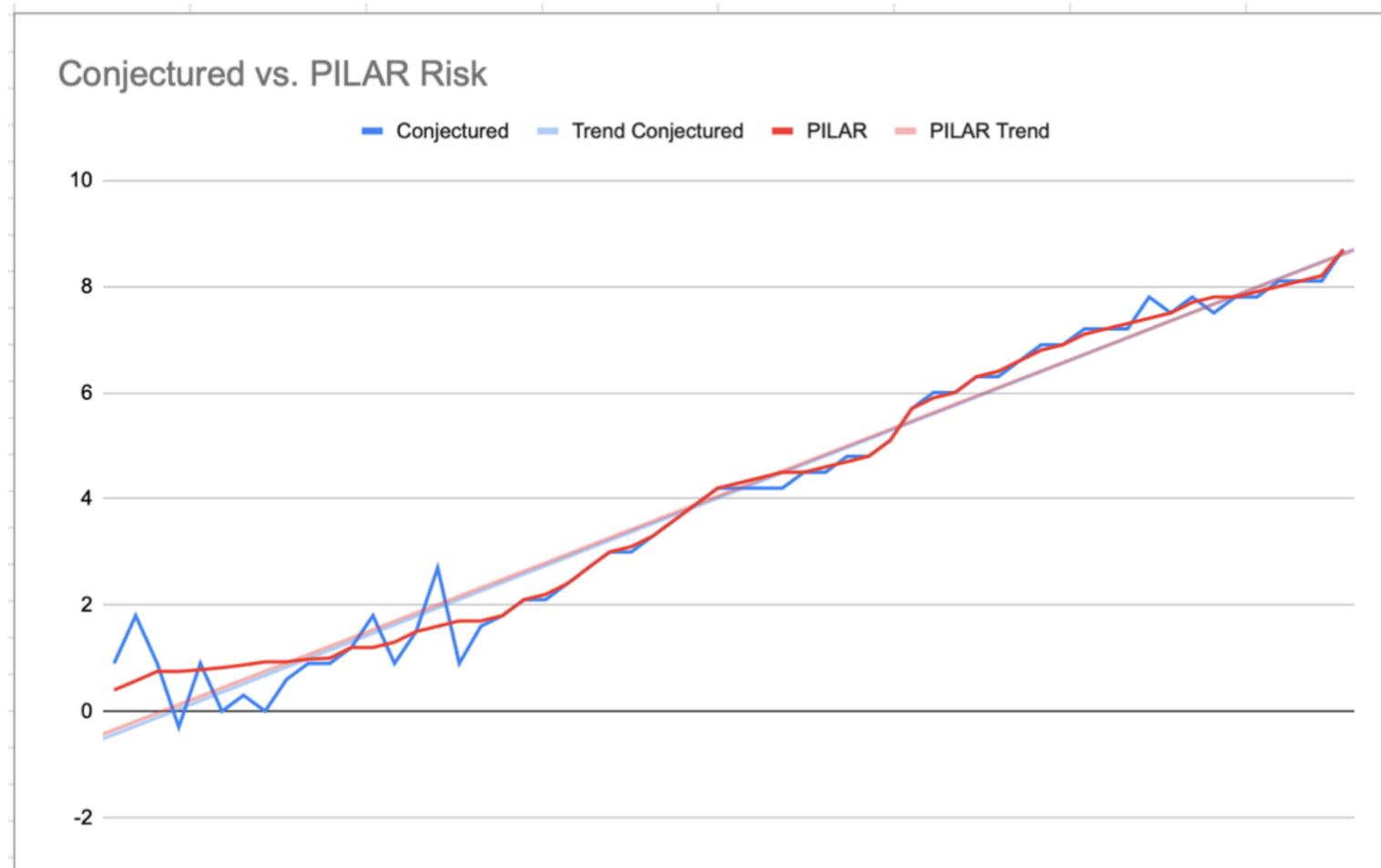
PILAR Heat Map

Risk	-0,9	0	0,9	1,8	2,7
10	5,1	6	6,9	7,8	8,7
9	4,5	5,4	6,3	7,2	8,1
8	3,9	4,8	5,7	6,6	7,5
7	3,3	4,2	5,1	6	6,9
6	2,7	3,6	4,5	5,4	6,3
5	2,1	3	3,9	4,8	5,7
4	1,5	2,4	3,3	4,2	5,1
3	0,9	1,8	2,7	3,6	4,5
2	0,3	1,2	2,1	3	3,9
1	0	0,6	1,5	2,4	3,3
0	0	0	0,9	1,8	2,7

PILAR Conjectured Map

PILAR Reverse Engineering

Linear fit $y = 0.97x + 0.15$ with $r = 0.9909792073$



STRIDE Methodology

Spoofing identity

- Illegally accessing and then using another user's authentication information

Tampering with data

- Malicious modification
- Unauthorized changes

Repudiation

- Deny performing an malicious action
- Non-repudiation refers to the ability of a system to counter repudiation threats



Elevation of privilege

- Unprivileged user gains privileged access to compromise the system
- Effectively penetrated and become part of the trusted system

Denial of service

- Deny service to valid users
- Threats to system availability and reliability

Information disclosure

- Exposure of information to individuals not supposed to access

Case Study: Automotive Overview

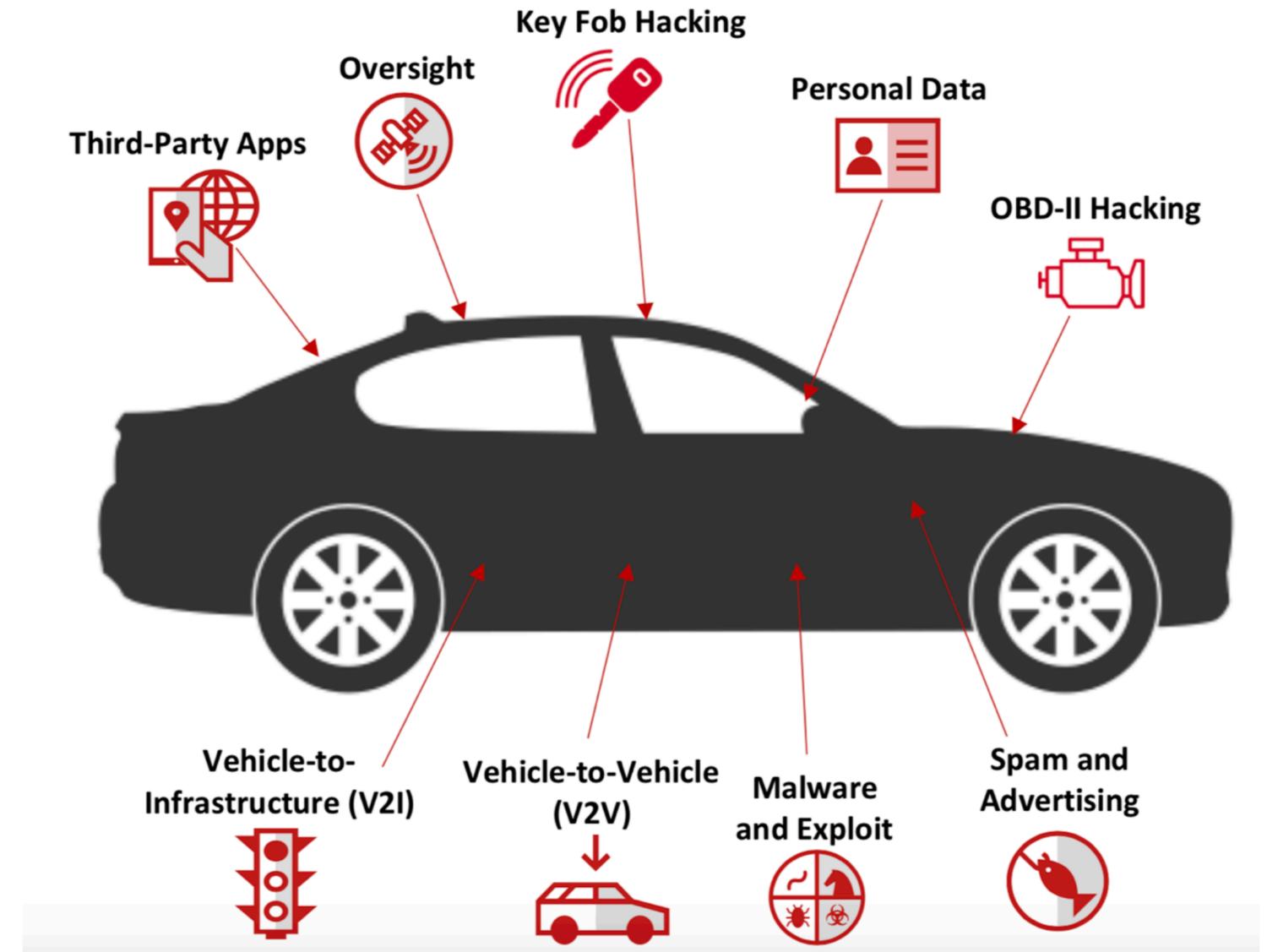
ANDY GREENBERG SECURITY 03.05.2020 07:00 AM

Hackers Can Clone Millions of Toyota, Hyundai, and Kia Keys

Encryption flaws in a common anti-theft feature expose vehicles from major manufacturers.

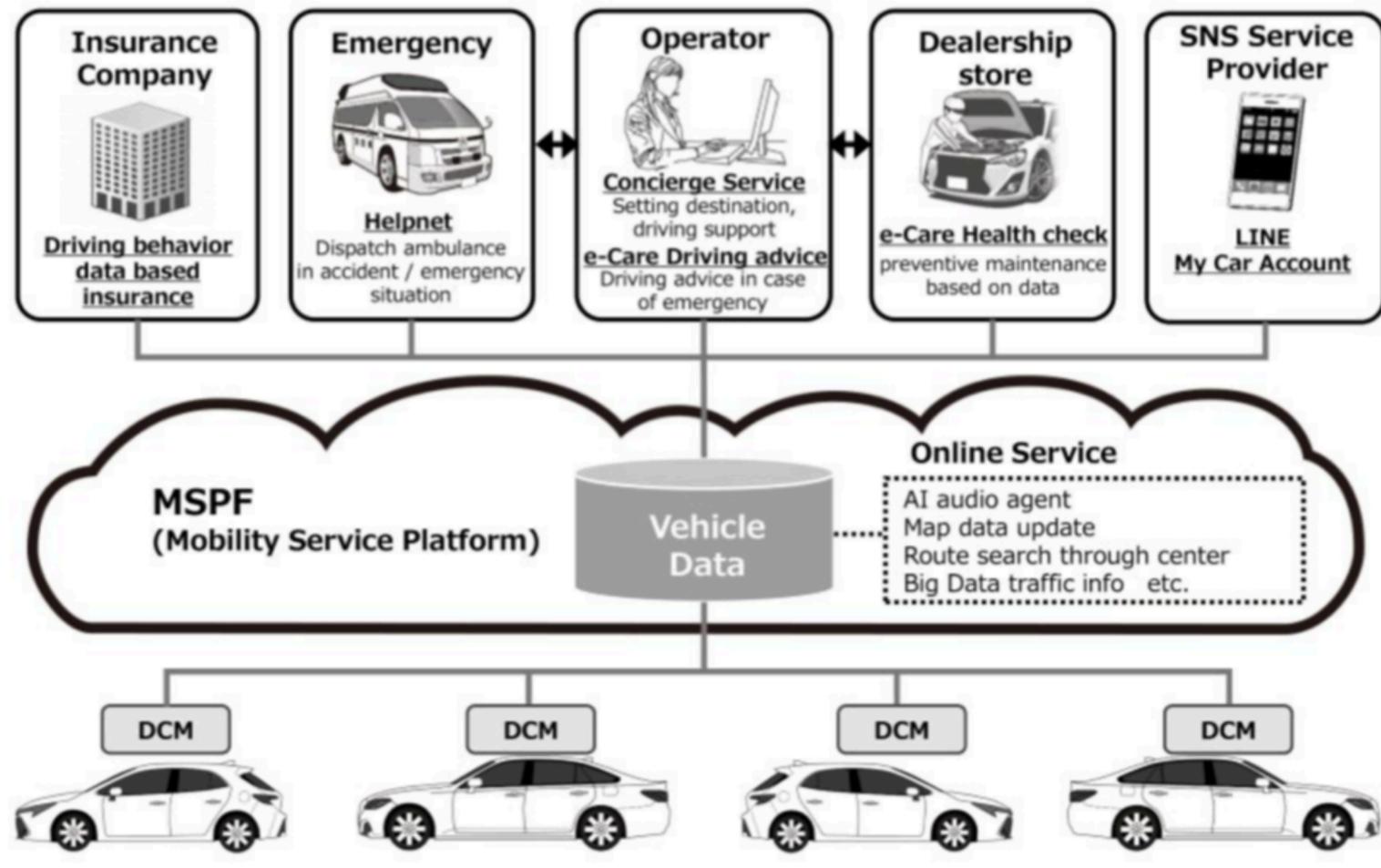


Source: Wired

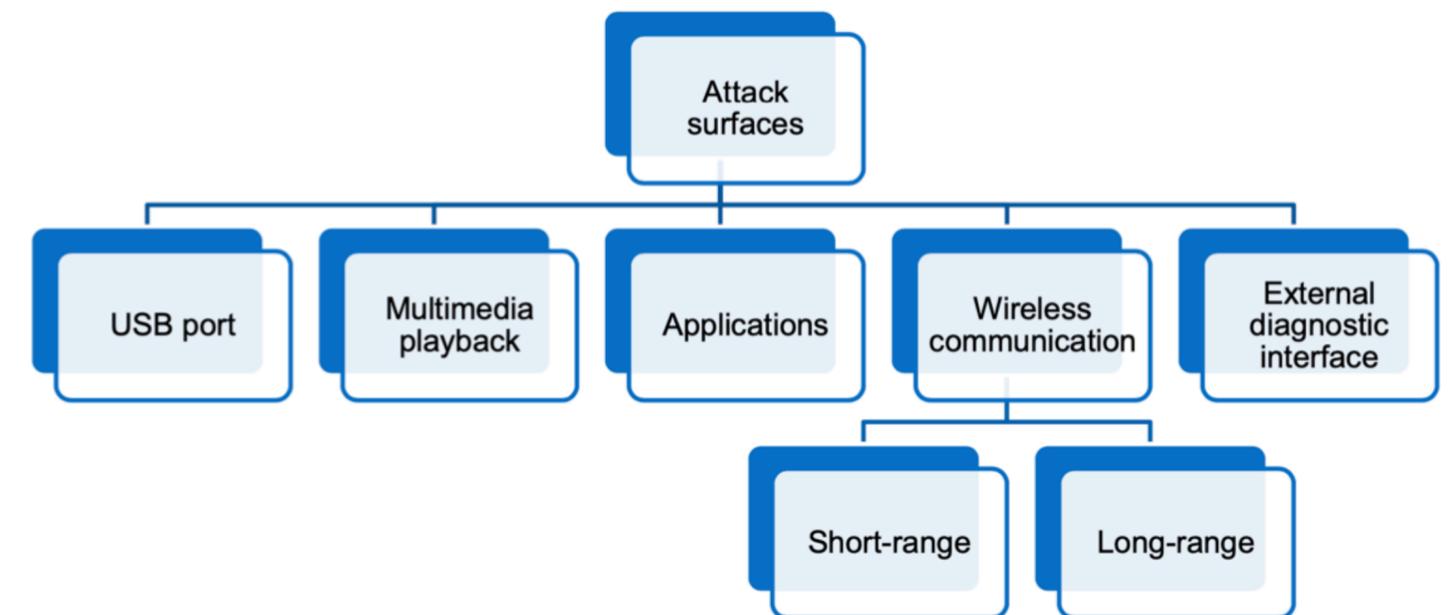


Source: McAfee

Case Study: Automotive Overview



Source: Toyota



Source: ALS19

Case Study: Threat Modeling and PILAR Demo

Threats Class 1 (T1): Authentication				
ID	Description	TA	STRIDE	Impact
T1.1	Customer identity loss or identity sharing: users leave their login credentials on a public place (e.g., write them down on a piece of paper) or share them with family, friends or relatives.	TA1.1	S	Low
T1.2	Personnel identity loss or identity sharing: personnel users and/or system admins leave their login credentials in public places or share them with others.	TA2.1, TA3.1, TA3.2	S	High

Threat Agents:

- ▶ Customer (TA1)
- ▶ Personnel (TA2)
- ▶ Administrator (TA3)
- ▶ Adversary (TA4)

The screenshot displays the AURA tool interface for threat modeling. The main window is titled "[AURA01] A.2. Threats > A.2.2. identification". It features a "Layers" tab with sub-tabs for "Assets", "Domains", and "Statistics".

The "ASSETS" tree on the left is organized as follows:

- [CA] Car
 - [CASW] Software
 - [APP] Applications
 - [MSP] Mobility Service Platform
 - [AHUF] Automotive Head Unit Firmware
 - [COM] Communications
 - [CAN] CAN Bus
 - [DCM] Data Communication Module
 - [GPS] GPS
 - [BT] Bluetooth
 - [WF] WiFi
 - [MC] Mobile Connection (4G/5G)
 - [DSWA] DSRC/WAVE
 - [CAHW] Hardware
 - [AHU] Automotive Head Unit
 - [USB] USB
 - [MP] Multimedia Playback
- [CO] Company
 - [COSW] Software
 - [ISWS] IS Web Server
 - [ISDB] IS Database
 - [DSHCWS] DSHC Web Server
 - [DSHCDB] DSHC Database
 - [EHWS] EH Web Server
 - [EHDB] EH Database
 - [COHW] Hardware
 - [PD] Personnel's devices
 - [CDATA] Data
 - [CMAC] CMA authentication credentials
- [BA] Base
 - [DATA] Data
 - [CDA] Customer data

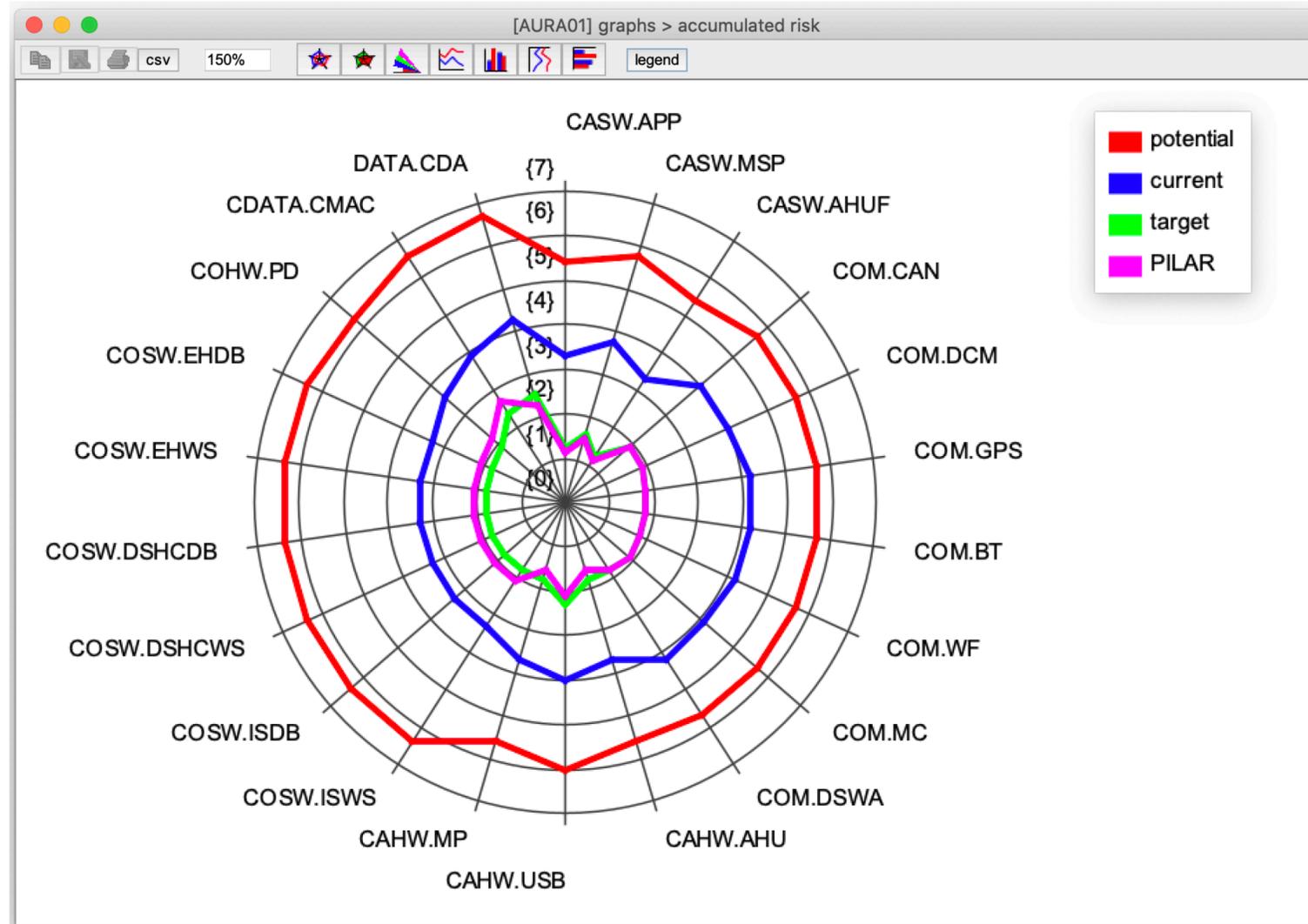
The "TSV" (Threat Statement View) pane on the right shows a list of threats, each with a red triangle icon indicating severity. The threats listed include:

- [I.5] Hardware or software failure
- [I.9] Interruption of other services or essential supplies
- [E.1] User errors
- [E.2] System / Security administrator errors
- [E.8] Malware diffusion
- [E.15] Accidental alteration of the information
- [E.18] Destruction of information
- [E.19] Information leaks
- [E.20] Software vulnerabilities
- [E.21] Defects in software maintenance / updating
- [E.24] System failure due to exhaustion of resources
- [A.5] Masquerading of identity
- [A.6] Abuse of access privileges
- [A.7] Misuse
- [A.8] Malware diffusion
- [A.11] Unauthorised access
- [A.13] Repudiation (denial of actions)
- [A.15] Deliberate alteration of information
- [A.18] Destruction of information
- [A.19] Disclosure of information
- [A.22] Software manipulation
- [A.24] Denial of service

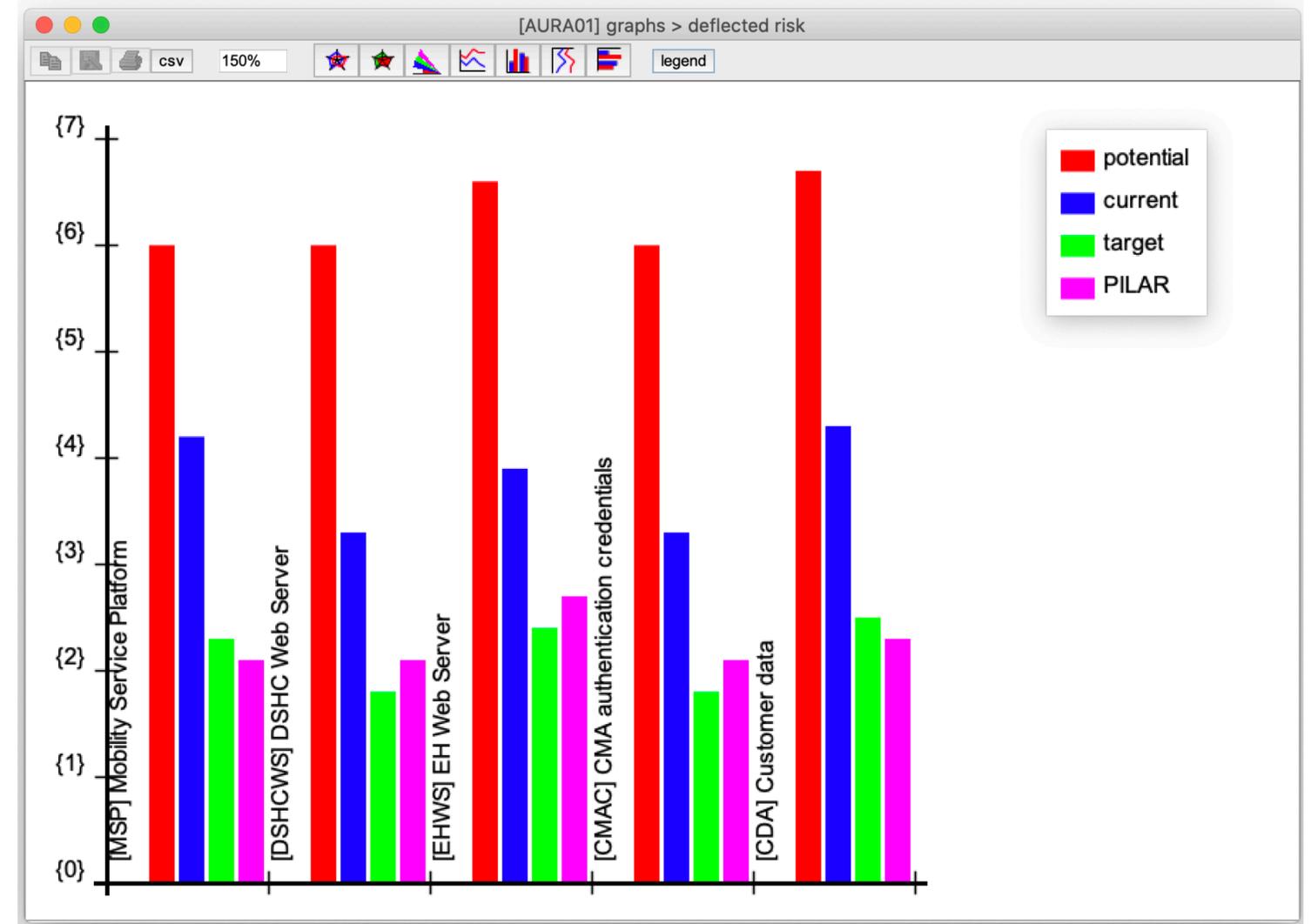
On the far right, a "THREATS" summary pane lists categories with red triangle icons:

- [N] Natural
- [I] Industrial
- [E] Errors and unintentional
- [A] Willful attacks
- [PR] Privacy risks

Case Study: PILAR Results



Accumulated Risk



Deflected Risk

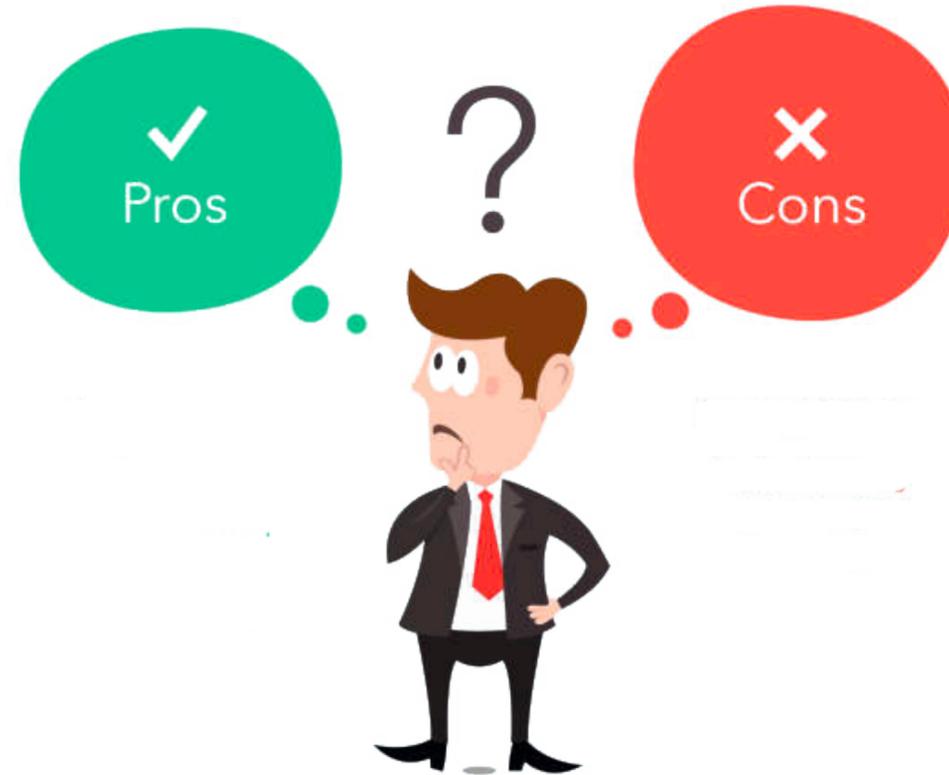
Conclusions

Magerit Pros:

- General methodology
- Compliance to international standards
- Threat Modeling integration (STRIDE)

Pilar Pros:

- Support to libraries (GDPR, ISO 27002)
- Assets/Threats classification
- Frequently updated



Magerit Cons:

- Variation of ISO 27005, without Pilar

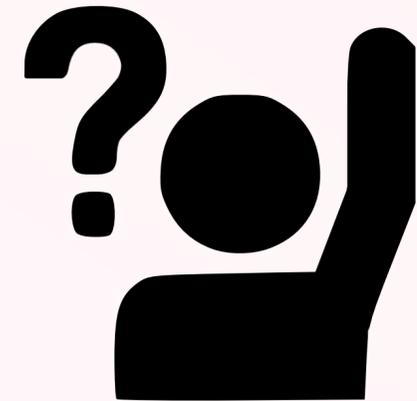
Pilar Cons:

- Granularity*
- Repetitive and confusing
- Unknown algorithms implementation

Future work and improvements:

- Further investigations (Pilar)
- Comparison with other methodologies and tools
- DPIA integration (GDPR)
- Risk Treatment

AUtomotive Risk Assessment



Q&A
