DIPARTIMENTO
di MATEMATICA
e INFORMATICA

CORSO DI LAUREA MAGISTRALE IN INFORMATICA

UNIVERSITÀ DEGLI STUDI DI CATANIA

AURA

AUtomotive Risk Assessment

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

MARIO RACITI

MASTER'S THESIS

SUPERVISOR:
PROF. GIAMPAOLO BELLA

ACADEMIC YEAR 2019/2020

To my love Vincenza

Acknowledges

I would really like to thank my supervisor Prof. Giampaolo Bella for the enormous support, patience, availability and for believing in me. It has been for me (and continues to be) a source of inspiration and has ignited in me the desire and strength to move forward in this work and deepen more and more cybersecurity. I really thank my wonderful girlfriend Vincenza, to whom I dedicate this work, for always supporting me, especially in the realisation of this thesis, and for always supporting me even in the most stressful phases of this path. Furthermore I would also like to thank Dr. Federico Fausto Santoro for the continuous support, inspiration and for having always believed in me, and Dr. Eva Sciacca and Dr. Fabio Vitello from INAF for the internship opportunity. In general I would like to thank all the professors from DMI, but above all I would like to mention those who have always encouraged me in my studies and taught a lot: Prof. E. Tramontana, Prof. S. Riccobene, Prof. M. Madonia, Prof. C. Santoro, Prof. G. Pappalardo. Also I would like to thank Andrea Menin who is a source of inspiration for me and has given me the opportunity to share my cybersecurity studies in his fantastic blog. Special thanks also to my colleagues and former colleagues, as well as friends, Francesco, Samuele, Salvatore, Giuseppe, Nicola, Giammarco, Gioele, Marco, Enrico, Mirko and Nunzio, who have supported me in these years of study and have had the patience to encourage me. They, in particular, helped me in various difficulties and always gave me advice for any type of problem. Last but not least, I would also like to take this opportunity to thank my parents who allowed me to achieve this goal and most of all my brother Lorenzo, for the motivation and support he gives me every day and for always being there when I needed it. Finally, I also thank you in advance who will want and kindness to read this work.

Preamble

The present work is the result of my own studies and continuous research, except where stated. The main source for the information reported in this thesis refer to the official website of the European Union Agency for Cybersecurity (ENISA). The description of the Risk Assessment process refers to the official ISO/IEC 27005:2018 standard.

The version of the methodology described and adopted is MAGERIT v3. Its description refers to all of the three official books, id est, "Book I: Methodology", "Book II: Catalogue of elements", "Book III: Practical techniques". Furthermore, as the last two books of the current version of the methodology are only available in Spanish, the information included in this work referring to them was translated as well as summarised. The version of the tool used is PILAR 7.4.4. Since the latter is a commercial tool, an evaluation license was used, allowing free use of Pilar for a period of 30 days. As these days sufficed to perform the risk assessment exercise, it was not necessary to apply for an educational license. All of the resources referring to Magerit and Pilar are freely available on the official website of EAR/PILAR.

The case study presented in this work refers to an article published by Toyota Motor Corporation. It was chosen this example because it offers a good outline of the state of the art technology in the automotive field, thus it well suited — although some changes had to be done — the requirements for the risk assessment exercise. For this reason, some of the terms used may purely refer to products owned by Toyota, but the basic concepts remain generic and comparable to any other example. Moreover, the threats presented in the case study scenario allude to the common attacks against car infotainment systems with particular attention to data privacy and communication components.

Abstract

Over the last few years the increasing of electronic and digital components in cars has improved the safety and driving experience of the vehicles. Although, the higher number of externally-communicating units has led to a growth in the dimension of the attack surfaces of each vehicle and, consequently, novel cybersecurity risks and threats are arising. Since smart cars are increasingly complex and involve multiple components, appropriate security measures need to be implemented to mitigate the potential risks, especially as attacks threaten the security, safety and even the privacy of vehicle passengers and all other road users, including pedestrians.

In this work we propose a Risk Assessment exercise applied to an automotive scenario, according to the MAGERIT methodology and with the support of the PILAR/EAR commercial tool, in order to seek whether both the methodology and the tool may prove to be useful in the automotive field, with specific attention paid to communication peripherals and cloud, which may potential threaten personal data en route from/to connected vehicles. For this purpose, we introduce an overview of the Risk Assessment process according to ISO/IEC 27005, followed by a description of Magerit. Moreover, we also provide a regression analysis study of the algorithm implemented in Pilar for the purposes of reverse engineering, to better understand the values calculated by the tool in the demo. The latter follows a description of the case study within a STRIDE threat modeling analysis preparatory to the demo itself.

Contents

List of Tables

List of Figures

1 Introduction

In recent years, the need to manage risk in a structured and rigorous manner, integrated into governance, planning, strategies, policies, values and the overall corporate culture, has grown steadily. This is mainly due to the fact that companies in continuous evolution involve increasingly articulated and complex risks, such as to compromise the achievement of strategic, economic and financial objectives. Nevertheless, it has always been known that conducting business involves risk as Gary Cohn, an American business leader, stated:

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

Technology is driving unprecedented disruption in the industry, especially in the automotive market. The automotive industry comprises a wide range of companies and organisations involved in the design, development, manufacturing, marketing, and selling of motor vehicles and, thus, it is one of the world's largest industries by revenue. Automotive will become more diversified as new business models and different technological expertise enter the field. A shift to a more digitised and consumer-focused market, however, means that automotive companies will have to face a new type of risk. In addition to the classic risks concerning the "car" product, indeed they should deal with risks deriving from the Information and Communication Technology (ICT) field. Among these, we can recall the problem of privacy which for instance, with the entry into force of the European General Data Protection Regulation (GDPR)[1], could represent a critical factor in terms of compliance. In this regard, it should be recalled that in the automotive field (and not only) personal data are exposed to risks due to the growth of Internet of Things (IoT) smart devices and the emerging use of the cloud.

As a result with this increased connectivity — also the advancement of 5G is expected to further promote it — novel cybersecurity risks and threats arise and, consequently, there is the need to manage them. In addiction, the potential attack surface and attack vectors are also expanded with the emergence of semi-autonomous and autonomous cars, which make use of advanced machine learning and artificial intelligence techniques. Another factor which leverages the increase of risks can be ascribed to the deployment of intelligent transport systems and autonomous cars, i.e., Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) interfaces.

Since smart cars are increasingly complex and involve multiple components, appropriate security measures need to be implemented to mitigate the potential risks, especially as attacks threaten the security, safety and even the privacy of vehicle passengers and all other road users, including pedestrians. For this purpose, an Information Security (IS) Risk Assessment (RA) process helps in detecting and alleviating the security risks threatening an organisation — RA can be employed also to specific components or products. In general, Risk Assessment aims to measure the security posture of the organisation, checking whether the organisation is compliant with requirements and industry frameworks. These practices control and assess open ports, antivirus updates, password policies, patch management, encryption strength and so forth. This way, the cybersecurity professionals within an organisation can clearly see the efficiency of the organisation's controls, determine risk factors, come up with detailed plans and solutions, detect vulnerabilities and offer options to alleviate them.

1.1 Summary of Works

After a brief introduction, the text starts with a chapter discussing on the Risk Management/Risk Assessment **state of the art**, which aims to provide a broader vision of the most known RM/RA different methodologies and their applications. It follows a chapter regarding **Risk Assessment according to ISO/IEC 27005** in order to frame this concept in the wider Risk Management context and to provide a description of the RA phases as well as an appropriate terminology, that is also preparatory to the next chapters.

Successively, the concept of **Threat Modeling** is outlined with specific attention to the **STRIDE methodology**. The reason behind the composition of this chapter lies on the fact that threat modeling is very useful in a Risk Assessment process, as it may be seen as integral part of the Risk Analysis phase, and it particularly useful in the identification step. Nevertheless the STRIDE methodology is applied to the case study since it is compatible with the MAGERIT methodology — which is chosen for the Risk Assessment exercise since it claims to be generic and comes with a support tool —, thereby it is appropriate to describe this method before employing it.

Afterwards, a chapter about **the MAGERIT methodology and the PILAR tool** is introduced, as they are chosen for conducting the Risk Assessment exercise. In particular, this part is necessary to understand some glossary diversities between the MAGERIT methodology (and Pilar) and ISO 27005 — although the former is compliant with the latter as also mentioned in the relative section.

Furthermore, the next chapter, which is the more peculiar, deals with a **Regression Analysis for the purposes of Reverse Engineering** of the PILAR tool. Since the latter is a commercial tool, it is not specified what algorithms, heuristics and formulas it implements. Thus, this chapter aims to understand how the tool calculates the values of risk and impact by performing empiri-

cal experiments and, then, by applying a regression analysis to the empirical values to estimate, in this case, an exponential fit for impact and a linear fit for risk. Consequently, here it also attempts to justify the results of the demo presented in the following chapter.

Speaking of demo, next it is indeed provided a series of sections about the **case of study**, within an outline about automotive security risks and a description of the case study. The latter is highly inspired to an article published by Toyota Motor Corporation, as it offers a good outline of the state of the art technology in the automotive field. It follows a section about the Risk Assessment exercise applied to the case study, which starts with a **STRIDE threat modeling** for the identification phases (also involved by Magerit) and terminates in a **demo** within the tool.

Eventually, the conclusive chapter discusses about the results, pro and cons of both the methodology and the tool, and suggests some future works.

2 State of the Art

In the Information Technology (IT) Security literature there are several Risk Management/Risk Assessment methodologies and frameworks suitable for different cases. Indeed, RM/RA can be employed in different fields and in different manners. Classically these processes are adopted within companies but over time, both general and targeted methodologies and frameworks have been designed. While it is possible to adopt a Risk Management/Risk Assessment process for the IT infrastructure of a company or a public body, it is also possible to use a (probably) different methodology to be able to perform the same work on, for example, a supply chain, about a particular product or software development cycle.

Below we present a collection of both standards and methods that better represent the state of the art. Note that these descriptions refer to the official documentations of the methodologies and ENISA[2]. In particular, the latter already offers an objective overview of these methodologies, so it has been convenient to report their summaries.

2.1 ISO 27005 Framework

ISO/IEC 27005[3] is the international standard that describes how to conduct an information security risk assessment in accordance with the requirements of ISO/IEC 27001. Its main objective is to improve Information Security Management Systems (ISMS) in any company or organisation. Additionally, it implies a specific methodology for each information security problem. Companies and organisations with ISMS problems may focus on the individual factors, such as the actual scope of the ISMS or commercial sector of the industry itself, rather than applying the entire methodology of the standard.

ISO 27005 is a generic framework applicable to all organisations, regardless of size or sector. It is designed to assist the satisfactory implementation of information security based on a risk management approach. Unlike other popular risk management standards that adopt a one-size-fits-all approach, ISO 27005 is flexible in nature and allows organisations to select their own approach to risk assessment based on their specific business objectives.

This framework follows a simple, repeatable structure with each of the main clauses organised into the following four sections:

- Input: the information necessary to perform an action.
- Action: the activity itself.
- Implementation guidance: any additional detail.
- Output: the information that should have been generated by the activity.

This consistent approach helps to ensure that organisations have all the information required before beginning any risk management activity.

2.2 NIST SP 800-30 Framework

NIST SP 800-30, Guide for Conducting Risk Assessments[4], provides an overview of how risk management fits into the system development life cycle (SDLC) and describes how to conduct risk assessments and how to mitigate risks. It provides processes (tasks) for each of the steps in the Risk Management Framework at the system level. It gives very detailed guidance and identification of what should be considered within a Risk Management and Risk Assessment in computer security. There are some detailed checklists, graphics (including flowchart) and mathematical formulas, as well as references that are mainly based on US regulatory issues.

2.3 CRAMM Methodology

CRAMM[5] is a risk analysis method developed by the British government organisation CCTA (Central Communication and Telecommunication Agency), now renamed as Office of Government Commerce (OGC). This method comprises three stages, each supported by objective questionnaires and guidelines. The first two stages identify and analyse the risks to the system. The third stage recommends how these risks should be managed. The CRAMM method is rather difficult to use without the CRAMM tool. The first releases of both the method and tool were based on best practices of British government organisations. Currently, CRAMM is the UK government's preferred risk analysis method, but it is also used in many countries outside the UK, such as NATO, the Dutch armed forces, and corporations working actively on security, like Unisys. CRAMM is especially appropriate for large organisations, like government bodies and industry.

2.4 EBIOS Methodology

EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité - Expression of Needs and Identification of Security Objectives)[6] is

a method for analysis, evaluation and action on risks relating to information systems. It generates a security policy adapted to the needs of an organisation. The method was created in 1995 and is now maintained by the ANSSI, a department of the French Prime Minister.

The method provides five steps: Circumstantial study - determining the context; Security requirements; Risk study; Identification of security goals; and Determination of security requirements.

EBIOS is primarily intended for governmental and commercial organisations working with the Defense Ministry that handle confidential or secret defense classified information. It enables well informed security actions to be undertaken. The objective is to assess and prepare for possible future situations (in the case of a newly created information system), and identify and respond to deficiencies (when the system is operating) in order to refine the security arrangements.

In its first version, EBIOS was focused on "security objectives redaction". Since 2000, DCSSI became aware of improvements in international standards (ISO in particular) and "engaged EBIOS adaptation to this criteria". It might also be viewed as a way to avoid France's introspective approach to information security, responding to the limitations of French methods that are not recognised abroad and are unsuited to international markets. However, the method's documentation only appears to be available in French.

2.5 MEHARI Methodology

MEHARI (MEthod for Harmonised Analysis of RIsk)[7] is Risk Assessment and Risk Managemen method that also includes, directly in its knowledge bases, many formulas for the direct assessment of risk and selection of the ways to reduce them. MEHARI is not a pdf only method, it comes also as user friendly tool. Indeed, the knowledge bases are available as a workbook (for Excel or Open Office) capable to conduct the qualifica-

tion and quantification of all the elements of risk. This method enables business managers, information security/risk management professionals and other stakeholders to evaluate and manage the organisation's risks relating to information, information systems and information processes (not just IT). It is designed to align with and support information security risk management according to ISO/IEC 27005, particularly in the context of an ISO/IEC 27001-compliant Information Security Management System (ISMS) or a similar overarching security management or governance framework.

MEHARI has steadily evolved since the mid-1990s to support standards such as ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005 and NIST's SP 800-30.

2.6 MAGERIT Framework

Magerit[1] [8] is an open methodology for Risk Analysis and Management, developed by the Spanish Ministry of Public Administrations, offered as a framework and guide to the Public Administration. Given its open nature it is also used outside the Administration. Magerit is also compliant with several international standards, as ISO/IEC 31000:2009, ISO/IEC 27001:2005, ISO/IEC 15408:2005, ISO/IEC 17799:2005, ISO/IEC 13335:2004. Magerit v1 was published in 1997, Magerit v2 in 2005, whilst Magerit v3 was released in 2012. It is openly available in Spanish and English.

2.7 OWASP Framework

The OWASP Risk Assessment Framework[9] consists of Static Application Security Testing (SAST) and Risk Assessment tools. Even though there are many SAST tools available for testers, the compatibility and the environment setup process is complex. By using OWASP Risk Assessment Framework's Static Application Security Testing tool, testers will be able to

[1] This methodology will be deeply illustrated in Sec.5.

analyse and review their code quality and vulnerabilities without any additional setup.The framework can be integrated in the DevSecOps toolchain to help developers to write and produce secure code.

2.8 Standard of Good Practice for Information Security

The Standard of Good Practice for Information Security[10], published by the Information Security Forum (ISF), is a business-focused, practical and comprehensive guide to identifying and managing information security risks in organisations and their supply chains. The most recent edition is 2020, an update of the 2018 edition. Upon release, the 2011 Standard was the most significant update of the standard for four years. It covers information security 'hot topics' such as consumer devices, critical infrastructure, cybercrime attacks, office equipment, spreadsheets and databases and cloud computing. The 2011 Standard is aligned with the requirements for an Information Security Management System (ISMS) set out in ISO/IEC 27000-series standards, and provides wider and deeper coverage of ISO/IEC 27002 control topics, as well as cloud computing, information leakage, consumer devices and security governance.

In addition to providing a tool to enable ISO 27001 certification, the 2011 Standard provides full coverage of COBIT v4 topics, and offers substantial alignment with other relevant standards and legislation such as PCI DSS and the Sarbanes Oxley Act, to enable compliance with these standards too. The Standard is used by Chief Information Security Officers (CISOs), information security managers, business managers, IT managers, internal and external auditors, IT service providers in organisations of all sizes. The 2018 Standard is available free of charge to members of the ISF. Non-members are able to purchase a copy of the standard directly from the ISF.

3 Risk Assessment

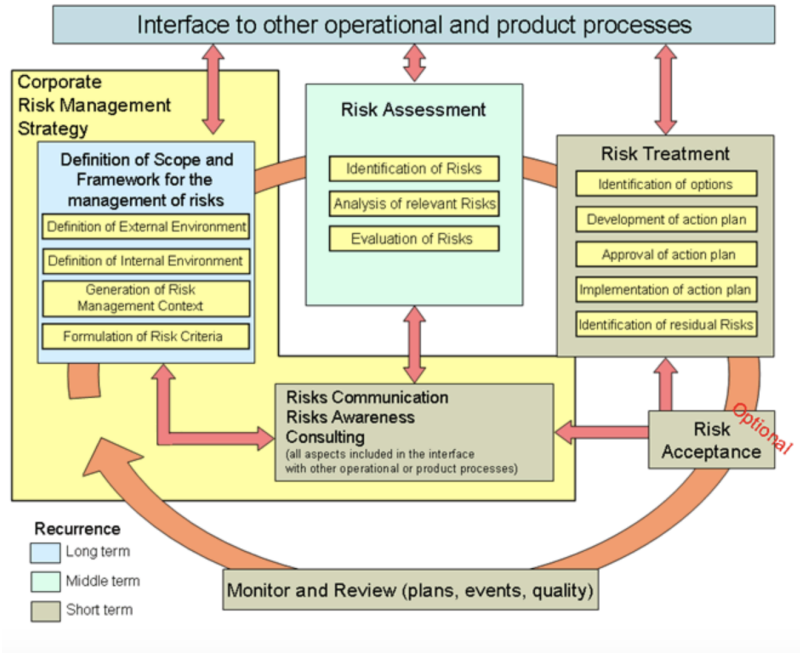


Figure 1: Risk Management Scheme (ENISA)

Risk Management (RM), in simple terms, is a process aiming at an efficient balance between realising opportunities for gains while minimising vulnerabilities and losses. It is an integral part of management practice and an essential element of good corporate governance[13]. Information Security (IS) Risk Management can be a part of an organisation's wider risk management process or can be carried out separately. Since Information Technology in general (and Information Security in particular), incorporates state of the art technology that is continuously changing and expanding, it is recommended that IS Risk Management is established as a permanent process within the organisation. Indeed, it is important to understand that **Risk Management should be seen as a cyclic process** in which, according to ISO/IEC 27001, we can identify several components, as depicted in Fig.1.

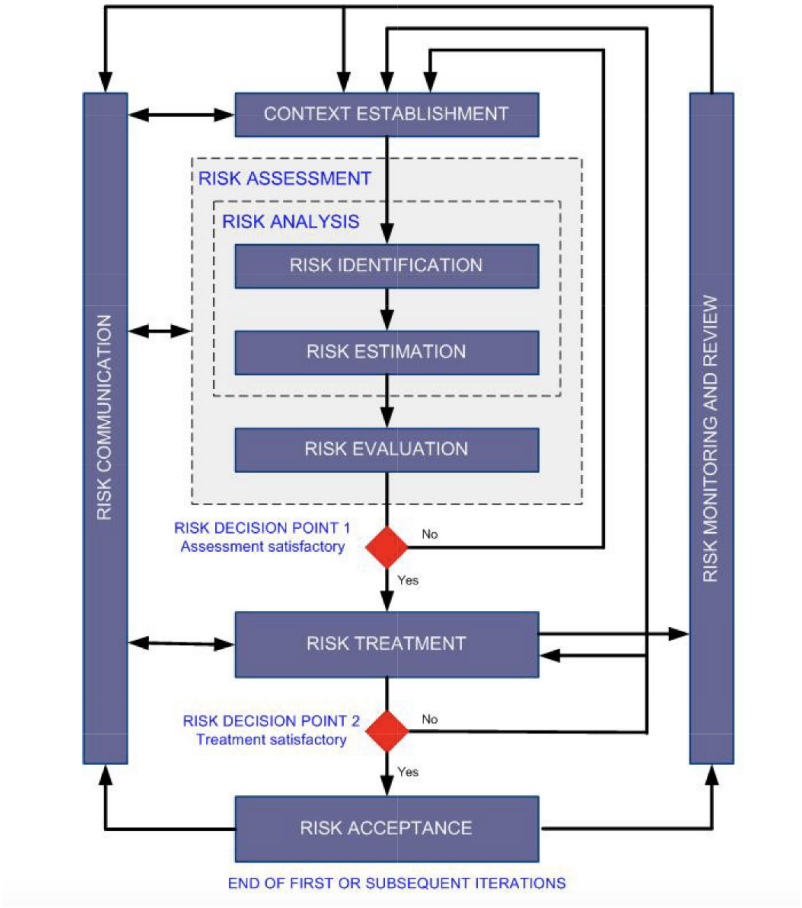


Figure 2: Risk Management Process [ISO 27005]

Despite ISO 27001 well summarises the Risk Management process within the foreseen scheme, it can be alternatively formalised by referring to ISO 27005. As a matter of fact, the latter is indeed a specific standard for Information Security Risk Management, thereby we will consider the topology depicted in Fig.2 as the default reference point from now on. Therefore, we can summarise **Risk Management** in three mainly parts: *Risk Assessment, Risk Treatment, Risk Acceptance*[3]. In particular, the former establishes what the organisation has at its disposal and calculates possible events, whereas Risk Treatment allows a thorough and sensible defence schema, preventing anything bad from happening and at the same time being prepared to tackle emergencies, survive incidents and continue operating under the best possible conditions. Eventually since nothing is perfect, risk is reduced to a residual level that is accepted by the Management (Risk Acceptance). Still according to ISO 27005, **Risk Assessment (RA)** can be further divided into three processes: *Risk Identification, Risk Estimation, Risk Evaluation*[3]. In addiction, we can clarify that the first two can also be gathered into a wider phase, the so called Risk Analysis. More specifically, Risk Assessment provides a model of the system in terms of assets, threats and safeguards[2] and is the foundation for controlling all activities on a well-founded base.

At this point it is important to note that Information security management systems (ISMS)[3] [ISO 27001] identify four main processes, which are illustrated in Fig.3. Risk Assessment is part of planning, where treatment decisions are taken. These decisions materialise in the implementation phase, when it is recommended to deploy some elements that allow controlling the measures implemented in order to assess their effectiveness and to act accordingly, within a framework of excellence or constant improvement.

[2] A definition of these elements is provided later.

[3] An ISMS is a set of policies and procedures for systematically managing an organisation's sensitive data, which goal is to minimise risk and ensure business continuity by

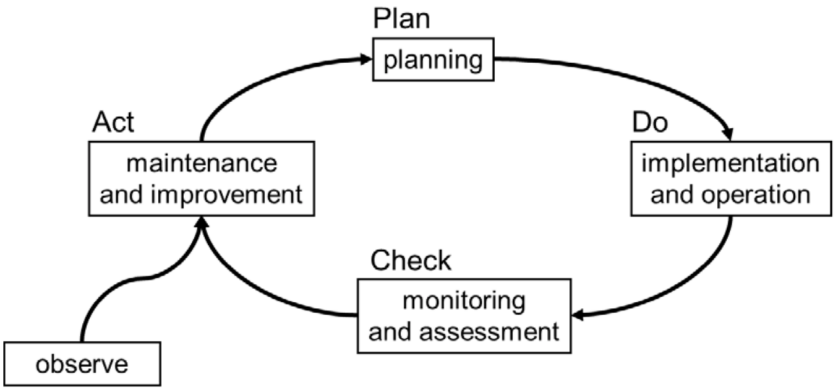


Figure 3: ISMS PDCA Cycle [ISO 27001]

Before continuing with the description of Risk Assessment phases, it is essential to recall some of the most relevant terms of the RM/RA glossary[14]. These are described in Tab.1 according to ISO/IEC and ENISA nomenclatures. Speaking of which, note that the Magerit glossary may be a bit different in some terms, thus the Magerit nomenclature will be clarified in its own time, in Sec.5 within a description of the methodology as well.

Glossary	
Term	Description
Asset	Anything that has value to the organisation, its business operations and their continuity, including Information resources that support the organisation's mission. (ISO/IEC PDTR 13335-1)
Threat	Any circumstance or event with the potential to adversely impact an asset through unauthorised access, destruction, disclosure, modification of data, and/or denial of service. (ENISA)

pro-actively limiting the impact of a security breach.

Threat Agent	An individual or group that can manifest a threat. It is fundamental to identify who would want to exploit the assets of a company, and how they might use them against the company.
Probability[4]	Extent to which an event is likely to occur. (ENISA)
Incident	An event that has been assessed as having an actual or potentially adverse effect on the security or performance of a system. (ENISA)
Vulnerability	The existence of a weakness, design, or implementation error that can lead to an unexpected, undesirable event compromising the security of the computer system, network, application, or protocol involved. (ITSEC)
Impact[5]	The result of an unwanted incident. (ISO/IEC PDTR 13335-1)
Safeguards[6]	Practices, procedures or mechanisms that reduce risk. (ISO/IEC PDTR 13335-1)
Mitigation	Limitation of any negative consequence of a particular event. (ISO/IEC Guide 73)
Risk	The potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organisation. (ISO/IEC PDTR 13335-1)

Table 1: Risk Management Glossary

[4]Also note as "likelihood". The likelihood of threat events resulting in adverse impacts estimates the possibility that a threat event would result in an actual outcome. The combined analysis of both threat assessment vectors impacts established an overall threat likelihood.

[5]The potential damage (physical, logical, monetary loss, etc) of a threat event.

[6]The term 'safeguard' is normally considered to be synonymous with the term 'control'.

In general threats can be of different origins. The information system is a passive victim of natural disasters (e.g., earthquakes, floods, etc.) and some industrial disasters (e.g., pollution, contamination, electric failures, etc.). In addiction to natural and environmental origins, there are problems caused by design and/or implementation failures that have negative consequences for the system — these are commonly called technical vulnerabilities or just 10 “vulnerabilities”. Accidental threats caused by people should also be considered, as people with access to the information system can cause unintentional problems, especially due to error or default. Eventually, people may deliberately cause threats: deliberate attacks either to get unfair advantage or with the intention of causing damages to the rightful owners.

As a summary, assets are subject to threats that, when do happen, degrade (the value of) the asset. The cost of a happening is called impact. If we are able to estimate the frequency of threat happenings, then tools can estimate the risk to which the system is subject. Degradation and frequency are the means to estimate the vulnerability of the system. System manager has an option to deploy safeguards, either to reduce the frequency, or to limit the impact. The degree of effectiveness of these safeguards makes the system subject to a residual risk.

In business words, from the foreseen factors, we can eventually summarise **risk** as "*the possibility that an event will eventually lead to reduced company profitability*".

3.1 Risk Analysis

Risk Identification and Risk Estimation are the main phases which characterise Risk Analysis, according to ISO 27005.

Good quality information and thorough knowledge of the organisation and its internal and external environment are very important in identifying risks. Historical information about this or similar organisations (competitors or not) may also prove very useful as they can lead to safe predictions about current and evolving issues that have not yet faced by the organisation. On the one hand, Risk Identification is the phase where threats, vulnerabilities and the associated risks are identified. This process has to be systematic and comprehensive enough to ensure that no risk is unwittingly excluded. It is very important that during this stage all risks are identified and recorded, regardless of the fact that some of them may already be known and likely controlled by the organisation. On the other hand, Risk Estimation is the phase where the level of the risk and its nature are assessed and understood. This information is the first input to decision makers on whether risks need to be treated or not and what is the most appropriate and cost-effective risk treatment methodology.

In general Risk Analysis involves thorough examination of the risk sources and their positive and negative consequences. It also takes into account the likelihood that those consequences may occur (and the factors that affect them) and the assessment of any existing controls or processes that tend to minimise negative risks or enhance positive risks[7].

The level of risk can be estimated by using statistical analysis and calculations combining impact and likelihood. Any formulas and methods for combining them must be consistent with the criteria defined when establishing

[7]These controls may derive from a wider set of standards, controls or good practices selected according to a an applicability statement and may also come from previous risk treatment activities.

the Risk Management context. This is because an event may have multiple consequences and affect different objectives, therefore consequences and likelihood need to be combined to calculate the level of risk. If no reliable or statistically reliable and relevant past data is available (kept for e.g. an incident database), other estimates may be made as long as they are appropriately communicated and approved by the decision makers.

Risk analysis may vary in detail according to the risk, the purpose of the analysis, and the required protection level of the relevant information, data and resources. Analysis may be qualitative, semi-quantitative or quantitative or a combination of these. In any case, the type of analysis performed should, as stated above, be consistent with the criteria developed as part of the definition of the Risk Management context.

In the chemical sciences, qualitative analysis is the process that aims to discover and isolate the elements or ingredients of a composite body. On the other hand, quantitative analysis is used to determine the amount of each element or ingredient.

Below we cite an overview of these different kind of analysis directly from an article by ENISA[15], which refers to ISO 27005 as well.

3.1.1 Qualitative Analysis

In qualitative analysis, the magnitude and likelihood of potential consequences are presented and described in detail. The scales used can be formed or adjusted to suit the circumstances, and different descriptions may be used for different risks.

According to ISO 27005, qualitative analysis may be used:

- as an initial assessment to identify risks which will be the subject of further, detailed analysis;
- where non-tangible aspects of risk are to be considered (e.g., reputation, culture, image, etc.);
- where there is a lack of adequate information and numerical data or resources necessary for a statistically acceptable quantitative approach.

3.1.2 Semi-Quantitative Analysis

In semi-quantitative analysis the objective is to try to assign some values to the scales used in the qualitative assessment. These values are usually indicative and not real, which is the prerequisite of the quantitative approach.

Therefore, as the value allocated to each scale is not an accurate representation of the actual magnitude of impact or likelihood, the numbers used must only be combined using a formula that recognises the limitations or assumptions made in the description of the scales used.

It should be also mentioned that the use of semi-quantitative analysis may lead to various inconsistencies due to the fact that the numbers chosen may not properly reflect analogies between risks, particularly when either consequences or likelihood are extreme.

3.1.3 Quantitative Analysis

In quantitative analysis numerical values are assigned to both impact and likelihood. These values are derived from a variety of sources. The quality of the entire analysis depends on the accuracy of the assigned values and the validity of the statistical models used.

Impact can be determined by evaluating and processing the various results of an event or by extrapolation from experimental studies or past data. Consequences may be expressed in various terms of the following impact criteria:

- monetary;
- technical;
- operational;
- human.

As it is made clear from the above analysis, the specification of the risk level is not unique. Impact and likelihood may be expressed or combined differently, according to the type of risk and the scope and objective of the Risk Management process.

3.2 Risk Evaluation

During the risk evaluation phase decisions have to be made concerning which risks need treatment and which do not, as well as concerning on the treatment priorities. Analysts need to compare the level of risk determined during the analysis process with risk criteria established in the Risk Management context (i.e., in the risk criteria identification stage). It is important to note that, in some cases, the risk evaluation may lead to a decision to undertake further analysis. The criteria used by the Risk Management team have to also take into account the organisation objectives, the stakeholder views and, of course, the scope and objective of the Risk Management process itself.

The decisions made are usually based on the level of risk, but may also be related to thresholds specified in terms of the following factors:

- *consequences* (e.g., impacts);
- the *likelihood* of events;
- the *cumulative impact* of a series of events that could occur simultaneously.

4 Threat Modeling

Threat modeling, combined with Risk Management/Risk Assessment, helps to give answers to the question like “Where am I most vulnerable to attack?”, “What are the most relevant threats?”, and “What do I need to do to safeguard against these threats?”. We can define threat modeling[17] as a process aimed to identify and enumerate potential threats (e.g., structural vulnerabilities, absence of appropriate safeguards) as well as prioritise possible mitigations.

Based on volume of published online content, below we quote the most well known methodologies according to Wikipedia and ThreatModeler[18]:

- *OCTAVE*. One of the first threat modeling methodologies created, Operationally Critical Threat, Asset, and Vulnerability Evaluation, focuses on assessing operational risk and security practices rather than technology. This methodology uses a self-directed approach, meaning creating and implementing security strategies falls directly on internal IT teams. OCTAVE threat modeling is useful for creating risk-aware corporate cultures.

- *STRIDE methodology*[8]. The STRIDE approach to threat modeling was introduced in 1999 at Microsoft, providing a mnemonic for developers to find ’threats to our products’. STRIDE, Patterns and Practices, and Asset/entry point were amongst the threat modeling approaches developed and published by Microsoft. References to "the" Microsoft methodology commonly mean STRIDE and Data Flow Diagrams.

- *PASTA* - The Process for Attack Simulation and Threat Analysis provides a seven-step process for aligning business objectives and techni-

[8]This methodology will be presented more in detail in the following section, as it will be adopted in Sec.7.3 for our case study.

cal requirements, taking into account compliance issues and business analysis. The intent of PASTA is to provide a dynamic threat identification, enumeration, and scoring process. Once the threat model is completed security subject matter experts develop a detailed analysis of the identified threats. Finally, appropriate security controls can be enumerated. This methodology is intended to provide an attacker-centric view of the application and infrastructure from which defenders can develop an asset-centric mitigation strategy.

- *Trike* - The focus of the Trike methodology is using threat models as a risk-management tool. Within this framework, threat models are used to satisfy the security auditing process. Threat models are based on a "requirements model." The requirements model establishes the stakeholder-defined "acceptable" level of risk assigned to each asset class. Analysis of the requirements model yields a threat model from which threats are enumerated and assigned risk values. The completed threat model is used to construct a risk model based on asset, roles, actions, and calculated risk exposure.

- *VAST*. This methodology is an acronym for Visual, Agile, and Simple Threat modeling. Automation, integration, and collaboration are the three pillars of scalable threat modeling that are fundamental to the VAST methodology. These processes help establish a sustainable self-service threat modeling practice driven by DevOps teams that scale across thousands of threat models. Specific security expertise is not required when creating or using these threat models due to unique application and infrastructure visualisation schemes like process flow diagrams.

4.1 STRIDE Methodology

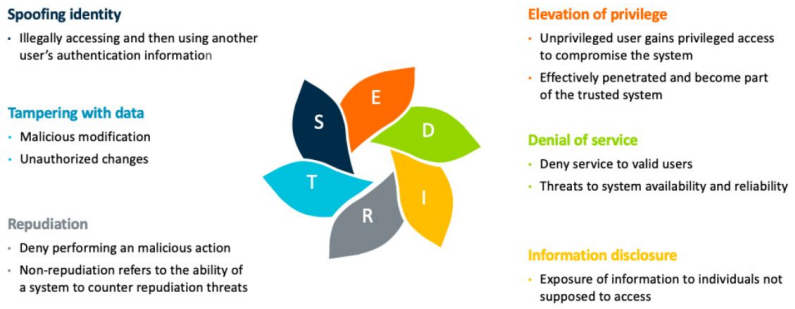


Figure 4: STRIDE Threat Model

The **STRIDE threat model**[19] approach developed by Microsoft Corporation can be used to expose security design flaws. This approach uses a technique called threat modeling which is based reviewing the system design in a methodical way. Threat modeling is processed in five steps[37]: (a) the identification of security objectives, (b) a survey of the application, (c) the decomposition of the application, (d) the identification of threats, and (e) the identification of vulnerabilities. Threat models, like the STRIDE approach, may often not prove that a given design is secure, but they help to learn from mistakes and avoid repeating them.

STRIDE is derived from an acronym for the following six threat categories:

- *Spoofing identity*. An example of identity spoofing is illegally accessing and then using another user's authentication information, such as username and password.
- *Tampering with data*. Data tampering involves the malicious modification of data. Examples include unauthorised changes made to persistent data, such as that held in a database, and the alteration of data as it flows between two computers over an open network, such as the Internet.

- *Repudiation*. Repudiation threats are associated with users who deny performing an action without other parties having any way to prove otherwise — for example, a user performs an illegal operation in a system that lacks the ability to trace the prohibited operations. Non-repudiation refers to the ability of a system to counter repudiation threats. For example, a user who purchases an item might have to sign for the item upon receipt. The vendor can then use the signed receipt as evidence that the user did receive the package.

- *Information disclosure*. Information disclosure threats involve the exposure of information to individuals who are not supposed to have access to it — for example, the ability of users to read a file that they were not granted access to, or the ability of an intruder to read data in transit between two computers.

- *Denial of service*. Denial of service (DoS) attacks deny service to valid users — for example, by making a Web server temporarily unavailable or unusable. You must protect against certain types of DoS threats simply to improve system availability and reliability.

- *Elevation of privilege*. In this type of threat, an unprivileged user gains privileged access and thereby has sufficient access to compromise or destroy the entire system. Elevation of privilege threats include those situations in which an attacker has effectively penetrated all system defenses and become part of the trusted system itself, a dangerous situation indeed.

5 MAGERIT Methodology

Figure 5: Magerit Logo

Magerit is an open methodology for Risk Analysis and Management, developed by the Spanish Ministry of Public Administrations, offered as a framework and guide to the Public Administration. Given its open nature it is also used outside the Administration.

According to ISO/IEC 31000 terminology[20], Magerit responds to what is called “Risk Management Process”, section 4.4 (“Implementing Risk Management”) within the “Framework for Risk Management”. In other words, MAGERIT implements the Risk Management Process within a working framework for governing bodies to make decisions taking into account the risks derived from the use of information technologies.

The ultimate aim of using Magerit is to make a methodical approach that leaves no room for improvisation, and not to depend on the analyst’s whim. Magerit is compliant to the following international standards: ISO 31000:2009, ISO 27001:2005, ISO 15408:2005, ISO 17799:2005, ISO 13335:2004.

Magerit seeks to achieve the following objectives[21]:

Direct objectives:

- To make those responsible for information systems aware of the existence of risks and of the need to treat them in time.
- To offer a systematic method for analysing these risks.
- To help in describing and planning the appropriate measures for keeping the risks under control.

Indirect objectives:

- To prepare the organisation for the processes of evaluating, auditing, certifying or accrediting, as relevant in each case.

The current version of Magerit (v3) has been structured into three books. All of the three are available in Spanish, whilst the former is also available in English[9].

Book I: Methodology[21]. It describes the core steps and basic tasks to carry out a project for risk analysis and management; the formal description of the project; the application to the development of information systems and it provides a large number of practical clues, as well as the theoretical foundations, together with some other complementary information.

Book II: Catalogue of elements[22]. It provides standard elements and criteria for information systems and risk modeling: asset classes, valuation dimensions, valuation criteria, typical threats, and safeguards to be considered; it also describes the reports containing the findings and conclusions (value model, risk map, safeguard evaluation, risk status, deficiencies report and security plan), thus contributing to achieve uniformity.

[9]Magerit v2 books are all available in both Spanish and English.

Book III: Practical techniques[23]. It describes techniques frequently used to carry out risk analysis and management projects such as: tabular and algorithmic analysis; threat trees, cost-benefit analysis, data-flow diagrams, process charts, graphical techniques, project planning, working sessions (interviews, meetings, presentations), and Delphi analysis. The application of the methodology can be supported by the software PILAR/EAR, which exploits and increases its potentialities and effectiveness (PILAR is limited to the Spanish Public Administration. EAR is a commercial product).

Magerit also aims to achieve uniformity in the reports containing the findings and conclusions from a risk analysis and management project. These are illustrated in Tab.2.

More in detail, Magerit is a Risk Assessment Method phases supported. We can mainly distinguish five phases, which in turn are divided into other steps:

1. *Risk identification*. Assets identification, classification, dependencies between assets, and value.
2. *Threats*. Identification relationship with assets and evaluation of vulnerability.
3. *Safeguards*. Identification and evaluation. Tool support.
4. *Risk analysis*. Accumulated impact and risk. Deflected impact and risk. Tool support.
5. *Risk evaluation*. From technical risks into business risks.

MAGERIT Reports	
Term	Description
Value model	Description of the value of the assets for the organisation as well as the dependencies between the various assets.
Risk map	Summary of the threats to which the assets are exposed.
Statement of applicability	For a set of safeguards indicate which ones are applicable in the information system under study, and which ones are meaningless.
Safeguard evaluation	Evaluation of the effectiveness of the existing safeguards in relation to the risks systems face.
Risk status	Classification of the assets by their residual risk; that is, by what could happen, taking the safeguards used into consideration.
Vulnerabilities report	Absence or weakness of the safeguards that appear as appropriate to reduce the risks to the system.
Compliance	Meeting some requirements. Formal statement that it is in line and in accordance with the corresponding regulations.
Security plan	Group of security programs that put the risk treatment decisions into action.

Table 2: MAGERIT Reports

5.1 MAGERIT vs. ISO 27005

When illustrating the Risk Management/Risk Assessment processes in Sec.3, we have often referred to ISO 27005 as a cornerstone. For this reason it could be interesting to glance at a comparison between Magerit and ISO 27005. A map[24] of the latter to Magerit v3 is illustrated in Fig.6.

27005:2011	**magerit v3**
8.2 Risk identification	
8.2.1 Introduction to risk identification	
8.2.2 Identification of assets	RAM.11 – Identification of assets
8.2.3 Identification of threats	RAM.21 – Identification of threats
8.2.4 Identification of existing controls	RAM.32 – Evaluation of safeguards
8.2.5 Identification of vulnerabilities	RAM.21 – Identification of threats RAM.22 – Valuation of threats RAM.32 – Evaluation of safeguards
8.2.6 Identification of consequences	RAM.22 – Valuation of threats
8.3 Risk analysis	
8.3.1 Risk analysis methodologies	
8.3.2 Assessment of consequences	RAM.22 – Valuation of threats
8.3.3 Assessment of incident likelihood	RAM.22 – Valuation of threats
8.3.4 Level of risk determination	RAM.42 – Risk estimate
8.4 Risk evaluation	
9. Information security risk treatment	Magerit: 4. Risk management process
10 Information security risk acceptance	Magerit: 4.1.2 Risk acceptance
12 Information security risk monitoring and review	
12.1 Monitoring and review risk factors	
12.2 Risk management, monitoring, reviewing and improving	
B Identification and valuation of assets and impact assessment	
B.1 Examples of asset identification	
B.1.1 The identification of primary assets	essential assets
B.1.2 List and description of supporting assets	other assets
B.2 Asset valuation	dependencies asset valuation
B.3 Impact assessment	threat valuation: degradation

Figure 6: ISO 27005:2011 vs. MAGERIT v3

5.2 MAGERIT Risk Analysis

The MAGERIT methodology offers a collection of some techniques used in Risk Analysis and Management in its third book[23], which defines a *technique* as "a set of heuristics and procedures that help to achieve the proposed objectives". In particular, Magerit considers two macro categories of techniques: *specific techniques* and *general techniques*. According to Magerit, the former can be further divided in three subcategories:

- Tables;
- Algorithmic techniques;
- Attack trees.

whilst general techniques can be divided in:

- Graphic techniques;
- Work sessions;
- Delphi method.

Many of the foreseen subcategories are further forked.

In the following paragraphs an outline of the main techniques[10] is provided, also to better understand the work presented in Sec.6 and Sec.7.

[10]It should be noted that the qualitative analysis is deepened from a mathematical point of view, being the method used in the case study later. While other methods, such as quantitative analysis, are treated more briefly for a completeness of speech.

5.2.1 Table Based Model

Experience has shown the usefulness of simple analysis methods carried out through tables which, although not very precise, are able to identify the relative importance of the various assets subject to threats. Therefore, this method results more convenient when a general and immediate overview of the situation is needed.

Basically a table based analysis can be opted to calculate the roughly calculate impact and risk. Speaking of which, let the following scale be useful for assessing the value of assets, the magnitude of the impact and the magnitude of the risk: *VL (very low), L (low), M (medium), H (high), VH (very high).*

Impact can be calculated on the basis of simple double entry tables:

Impact		***Degradation***		
		1%	10%	100%
Value	VH	M	H	VH
	H	L	M	H
	M	VL	L	M
	L	VL	VL	L
	VL	VL	VL	VL

Figure 7: Impact Estimation (RA Table)

It is obvious that, for instance, assets with a very high impact rating (VH) should receive immediate attention, rather than assets with a medium one (M), and so on.

Risk can be calculated on the basis of impact and likelihood:

Risk		*Likelihood*				
		VL	L	M	H	VH
Impact	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

Figure 8: Risk Estimation (RA Table)

Thus, the levels of risk can be classified, in descending order, as follows: *critical (VH), important (H), significant (M), low (L), negligible (VL).*

5.2.2 Qualitative Model

A qualitative analysis, as already described in Sec.7.4.2, does not quantify resources more precisely than necessary, to make the components of the model relative.

In a risk analysis process it is essential to assess, at least relatively, the elements involved, id est, assets, the impact of threats and the risk involved. For this purpose, a scale of symbolic levels is used:

$$V = \{\ldots, v_0, v_1, \ldots, v_i, \ldots\} \tag{1}$$

The value 0 represents that it has absolutely no value. This series of levels satisfies the following properties:

- minimal element: $\forall i, 0 < v_i$
- total order: $\forall i, v_i < v_{i+1}$
- there exists a special element, v_0, which is ranked as "negligible"[11]

Informally, an asset is said to have "i points" to indicate that it has been assessed as v_i.

Each asset receives a **value** on the *V scale*. Assets are rated on each of the security dimensions. It is also important to establish whether an asset A depends, significantly, or not on another asset B. In other words, the **dependency between assets** is a Boolean value: yes or no. It is also important to note that this property is a transitive relation.

$$A \rightarrow B \tag{2}$$

$$(A \rightarrow B) \wedge (B \rightarrow C) \implies (A \rightarrow C) \tag{3}$$

[11] This negligible level establishes a subjective boundary between what is appreciable and should be of concern, and what is negligible and can be ignored. Values below v_0 will be neglected.

The transitive closure of direct dependencies between assets is therefore interesting:

$$A \implies C \iff \exists B, (A \implies B) \wedge (B \rightarrow C) \tag{4}$$

It means that A depends (indirectly) on C if and only if there is an asset B, so that A depends directly or indirectly on B and B depends directly on C.

Let $SUP(B)$ be the upper set of B, that is, the set of assets that depend directly or indirectly on B:

$$SUP(B) = \{A_i, A_i \implies B\} \tag{5}$$

The **accumulated value** on B is defined as the highest value between its own and that of any of its superiors:

$$accumulated\_value(B) = max(value(B), max_i\{value(A_i)\}) \tag{6}$$

The above formula states that the accumulated value on an asset is the highest of the values included, either of itself, or any one above it.

When an asset is threatened, a part of its value is lost. Intuitively, we speak of a "**percentage of asset degradation**", indicated as d, whose value is between 0% and 100% of lost. d is set as a real value between 0.0 (0% degradation) and 1.0 (100% degradation).

Accumulated impact of a threat on an asset is the measure of what a threat implies; that is, the loss of accumulated value. Note that impact is measured in the same units as value. If an asset has an accumulated value v and a percentage of degradation d, the impact value is calculated with a function that meets the following boundary conditions:

- $impact(0, 0\%) = 0$
- $impact(v, 0\%) = 0$

- $impact(v, 100\%) = v$
- $\forall d, v_i < v_j \implies impact(v_i, d) < impact(v_j, d)$
- $\forall v, d_i < d_j \implies impact(v, d_i) < impact(v, d_j)$

When the impact is at v_0 or less, it is said to be *negligible*.

Regarding **deflected impact** of a threat on an asset, if asset A depends on asset B, then the threats to B have repercussions on A. If B suffers a degradation d, the same happens to A, with the impact on A being the loss of the basic value. If A has an eigenvalue v_A, and B has an eigenvalue v_B, the impacts on A and B will be:

$$impact\_over\_A = impact(v_A, d) \tag{7}$$

$$impact\_over\_B = impact(v_B, d) \tag{8}$$

Also in this case, when the impact is at v_0 or less, it is said to be *negligible*.

Similar to assets values, to characterise the **likelihood of threats** a scale of symbolic values is used:

$$P = \{\ldots, p_0, p_1, \ldots, p_i, \ldots\} \tag{9}$$

The value 0 reflects the impossible event. The p_0 value reflects a negligible probability. In other words, we have a series of likelihood levels, which are the elements or atoms of analysis. This series of levels satisfies the following properties:

- total order: $\forall i, p_i < p_{i+1}$
- there is a singular element, p_0, which is called "negligible probability"

Finally, **risk** is measured by referring to the following scale of values:

$$R = \{\ldots, r_0, r_1, \ldots, r_i, \ldots\} \tag{10}$$

The value 0 reflects the nonexistent risk. Risk is a function of impact and likelihood:

$$risk = \Re(impact \times likelihood) \tag{11}$$

$\Re$ is a function that has to be defined in line with the following requirements:

- $\Re(0, p) = 0$
- $\Re(v, 0) = 0$
- grows with the value: $\forall p, v_i < v_j \implies \Re(v_i, p) < \Re(v_j, p)$
- grows with likelihood: $\forall v, p_i < p_j \implies \Re(v, p_i) < \Re(v, p_j)$

Risk can assume the value r_0, or even lower values. In this case we say that the risk is *negligible*.

In calculating the **accumulated/deflected risk**, the accumulated/deflected impact on the asset will be used.

When a threat is in force, a series of **safeguards** is implemented, whose efficiency, e, is a real value between 0.0 (no protection) and 1.0 (fully efficient safeguard). This value can be decomposed into an efficacy versus impact, e^i, and an efficacy versus likelihood e^p.

If the asset, without protection, could suffer a degradation d, thanks to the safeguards, the **degradation is reduced** to a residual value dr:

- $dr(0, e^i) = 0$
- $dr(d, 0) = d$
- $dr(d, 1) = 0$

Residual impact is calculated analogously to the impact, but using the residual degradation:

$$residual\_impact = impact(v, dr) \tag{12}$$

A perfectly effective safeguards package reduces the impact to a residual value v_0, that is, to the level of negligible. If the safeguards are insufficient, the impact will continue to be appreciable. The **accumulated residual impact** is calculated on the accumulated value, whilst the **deflected residual impact** is calculated on the basic value.

Similar to the impact, the likelihood of the threat on the asset is reduced to a residual value. If the likelihood was p, we have the following **residual likelihood**:

- $pr(0, e^p) = 0$
- $pr(p, 0) = p$
- $pr(p, 1) = 0$

Being e^p the effectiveness[12] of the safeguards mitigating the probability of the threat occurring.

Residual risk is the risk calculated from the residual frequency and impact:

$$residual\_risk = \Re(residual\_impact \times residual\_likelihood) \tag{13}$$

The **residual accumulated risk** is evaluated using the residual accumulated impact, whilst the **residual deflected risk** is evaluated using the residual deflected impact.

[12] Remember that this value is in range 0.0 (0% effective; that is, useless) and 1.0 (100% effective; that is, perfect).

As a summary, the **qualitative model** combines the following analysis parameters:

- rating the value of the asset through a discrete scale;
- rating the degradation posed by a threat as a percentage;
- rating the likelihood of a threat through a discrete scale;
- the integration of a package of safeguards;
- rating the efficiency of the safeguards through a percentage.

5.2.3 Quantitative Model

In this model, already outlined in Sec.3.1.3, we work with values that are real numbers, always greater than zero. The degree of dependency between assets is modeled as a continuum between 0.0 (independent assets) and 1.0 (absolutely dependent assets; what happens on the lower one has a decisive impact on the higher one). Both the value of the asset, basic or accumulated, as well as the impact of a threat when it occurs and the risk it poses are measured. While the **impact** measures the value of the potential misfortune, the **risk** weights that impact with the estimated likelihood of the threat. Impact measures the cost if it were to occur, while risk is the measure of exposure over a period of time.

If the valuation of the asset is economic (monetary cost that would mean its total and absolute loss), then the calculated impact is the cost induced by the threat, and the calculated risk is the amount to be expected as annual losses. Thus, the quantitative model makes it possible to compare the **expenditure on safeguards with the reduction in losses**.

The estimations of impact and residual risk incorporate the efficiency of the safeguards when dealing with a threat.

The **quantitative model** therefore combines the following analysis parameters:

- asset value calibration by means of a numerical quantity;
- calibration of the dependency between assets by means of a percentage;
- calibration of the degradation that poses a threat by means of a percentage;
- calibration of the likelihood of the threat by means of a frequency;
- structuring of a safeguards package;
- calibration of the effectiveness of safeguards by means of a percentage.

5.2.4 Graphic Model

Graphical representations can support the risk analysis phase as a support for presentations and decision making.

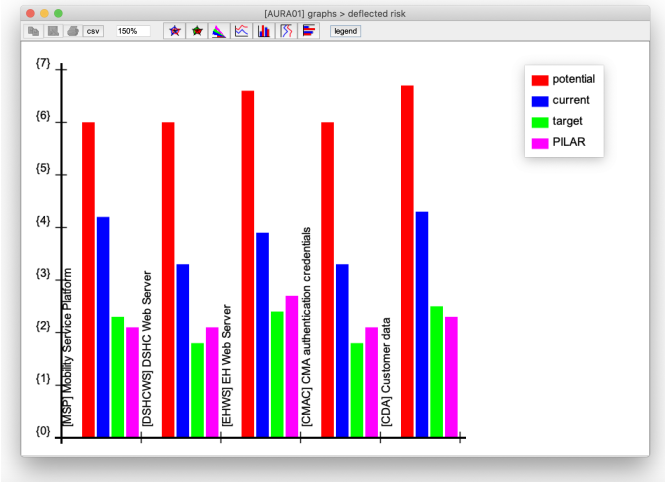


Figure 9: Example of Bar Diagram

Bar diagrams arrange the elements in conventional Cartesian coordinates: the elements to be considered on one axis and the values on the other axis. We can observe an example of bar diagram in Fig.9.

In this type of diagram it is easy to collect all the values. Sometimes horizontal level lines are introduced to mark thresholds: minimum or maximum values for some decision making. Informally, it can be said that they are presentations appreciated by people with a technical profile.

Radar charts represent the different variables or factors of the phenomenon under study on semi-axes or radii that start from a center. These radii, as many as factors, are graded to represent their levels and possible thresholds on a normal or logarithmic scale, as appropriate. Fig.10 illustrates an example of radar chart.

The value reached by each factor or variable is marked in its respective

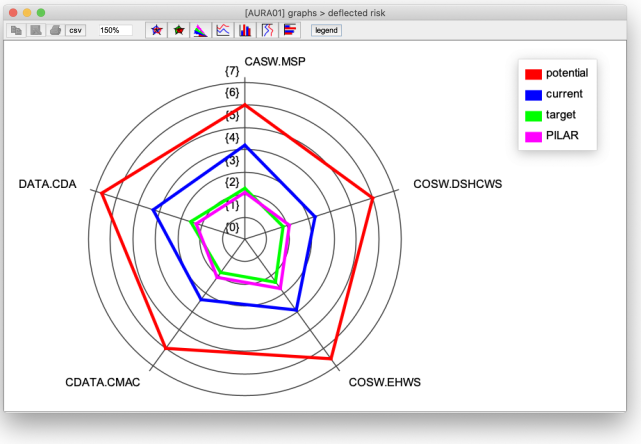


Figure 10: Example of Radar Chart

radius (the center represents the zero value). The consecutive points thus marked are joined by segments, corresponding to the values of the variables defined in the semi-axes, obtaining an irregular "starry" polygon called a *radar* or *wind rose* graph. All of them offer a synthetic vision of the phenomenon that allows to study it globally, facilitating the observation of its characteristics and tendencies as well as the balance between its different factors or elements. This synthetic vision is especially important in risk analysis and management, where a certain balance is sought between complementary factors. Security comes more from a homogeneous coverage without fissures than from a very high coverage in certain aspects against clear deficiencies in others seeking a certain compensation.

The basic radar chart requires you to begin by deciding which factors or variables to include. Thus, if one seeks to represent the global security state of an organisation, the factors will be the different services. After obtaining, calculating, classifying and tabulating the values of each factor, the scales are drawn as radii (within a great circle whose radius is the highest normalised value in each semi-axis). It is important to specify that there is the same angular distance between the semi-axes (i.e., they divide the

maximum circle into equal arcs).

Sometimes some levels (circles) are marked with special values such as minimum thresholds or maximum levels. Sometimes the covered area is filled in, but other times only the perimeter lines are painted. Surfaces are useful when it is not the case that one area "covers" another. The lines are always usable. These types of diagrams allow to:

- graphically synthesise balance or unbalance in various axes;
- accumulate profiles of highs or lows;
- show the temporal evolution.

Informally, it can be said that they are presentations appreciated by people with a managerial or management profile.

5.3 PILAR Tool

PILAR/EAR[25] is a commercial tool which provides a set of tools for analysis and management. It is specialised on Information and Communications Systems and supports the MAGERIT methodology provided by the Spanish Administration. It was partly funded by the Centro Criptológico Nacional (Spanish National Security Agency).

The tool provides a standard library for assets, threats and safeguards. Furthermore, it is able to derive security qualifications against widely known security standards, such as ISO/IEC 27002:2005 - Code of practice for information security management.

In Pilar some of the terms presented in the previous sections may be lexically different, thereby we provide the PILAR Glossary[26] in Tab.3.

It is important to note that the tool does not automate evaluation since this is a management activity. Instead, Pilar provides information on the risk level of each potential threat, both on each asset (accumulated risk level) and translated onto the essential assets of the organisation (deflected risk levels) with the corresponding backtracking to trace the point of attack onto the final consequences for the business. In other words, the tool provides detailed information on the facts. Therefore, it is the responsibility of the management team to interpret the consequences of incidents on the business.

Glossary	
Term	Description
Asset	Anything that has value to the organisation.
Attack	Attempt to destroy, expose, alter, disable, steal or gain unauthorised access to or make unauthorised use of an asset.
Availability	Property of being accessible and usable upon demand by an authorised entity.
Confidentiality	Property that information is not made available or disclosed to unauthorised individuals, entities, or processes.
Consequence	Outcome of an event affecting objectives.
Control	Means of managing risk, including policies, procedures, guidelines, practices or organisational structures, which can be of administrative, technical, management, or legal nature.
Integrity	Property of protecting the accuracy and completeness of assets.
Level of risk	Magnitude of a risk expressed in terms of the combination of consequences and their likelihood.
Likelihood	Chance of something happening.
Risk	Effect of uncertainty on objectives.
Threat	Potential cause of an unwanted incident, which may result in harm to a system or organisation effect of uncertainty on objectives.
Vulnerability	Weakness of an asset or control that can be exploited by one or more threats.

Table 3: PILAR RM Glossary

6 PILAR Reverse Engineering

Magerit is a methodology and sets down a number of axioms, but not algorithms. This is due to enable the tool(s) to improve heuristics over time, since there is no universal formulae to evaluate risk. Thereby, every tool does its best to make estimates that are useful to inform decisions related to security. Despite we outlined the qualitative risk analysis model more in detail in Sec.3.1.1 from a mathematical point of view, in this section we will try to better understand how the algorithms implemented in Pilar work. This work will also justify the values given in output by the tool in the demo presented in Sec.7.4.

It is essential to remark that Pilar is a commercial tool, thereby we have no access to the source code and, especially, its algorithms. We only know that it is a semi-quantitative tool and it supports Magerit. For this reasons the information provided below refers to a reverse engineering process consisting of empirical tests as well regression analysis approximations and conjectures on the potential[13] values of risk and impact.

6.1 Regression Analysis

In statistical modeling, regression analysis[28] is a set of statistical processes for estimating the relationships between a dependent variable (often called the 'outcome variable') and one or more independent variables (often called 'predictors', 'covariates', or 'features'). The most common form of regression analysis is linear regression, in which a researcher finds the line (or a more complex linear combination) that most closely fits the data according to a specific mathematical criterion. Regression analysis is widely used for prediction and forecasting. For this reason, it suits an important role in our attempt to understand the calculus of impact and risk in Pilar.

[13] This means that mitigating or aggravating conditions are not taken into account.

6.2 Impact Calculus

Pilar uses a table to map values with levels, shown in Tab.4, stored in a file named "levels.xml". As we can notice, three levels correspond to one order of magnitude. Thus, we can deduce that a 10% of degradation would mean decreasing the value of the asset by three steps.

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

Table 4: PILAR Levels Map

In Sec.3.1.1 we saw how Magerit basically defines the impact, saying it directly depends on asset value and degradation. Therefore, it was easy to discover that Pilar calculates impact exactly according the following equation:

$$I = (V \times d) \tag{14}$$

where I is the impact, V is the asset value in a specific dimension, d is

the degradation. Both I and V are expressed according their corresponding value in in the maps. Once the impact value has been calculated, we can retrieve its level thanks to an exponential fit — of course if this value is contained in the map, then we simply have its level by looking at the latter. With the help of some tools, such as WolframAlpha, it was possible to find an exponential function, which approximates the trend of the mathematical function with a reliability index of 99%, by providing as input the pairs of values indicated in the map[14]:

$$y = 1002.75e^{0.767241x} \tag{15}$$

This means that the function used by the tool is estimated, with an error equal to 1%, to that expressed in Eq.15. Thus for instance, given $V = 6(= 100000)$ and $d = 20\%$ we can calculate the impact by applying both Eq.14 and the foreseen exponential fit equation:

$$I = (V \times d) = 100000 \times 20\% = 20000 \simeq_{(15)} 3.9 \simeq 4 \tag{16}$$

In addiction, whether we are interested in calculating only the discrete value of the impact, it is possible to follow this reasoning: $d = 1\%$ means a decrease of the asset value of 6, $d = 10\%$ a decrease of 3, $d = 20\%$ a decrease of 2, $d = 50\%$ a decrease of 1 and $d = 100\%$ a decrease of 0.

[14]More in detail, "exponential fit $\{\{0,1000\},\{1,2150\},...,\{10,2150000\}\}$" was the input for WolframAlpha.

6.3 Risk Estimation

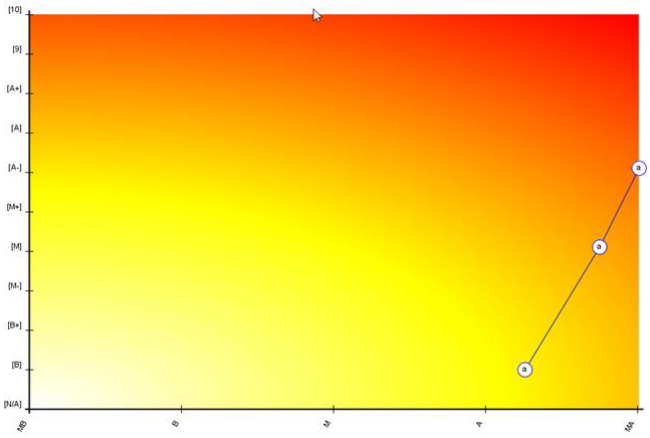


Figure 11: PILAR Heat Map

The calculus of risk is a bit more complicated than the impact case. As mentioned in Sec.3.1.1, risk is a result of impact and likelihood. In the prior section we explained the way Pilar calculates impact. Although, we do not know how it exactly quantifies likelihood. The official glossary[27] of the tool only states that Pilar uses a heat map, shown in Fig.11, to calculate the risk value and only states that:

"*[...] In a qualitative risk analysis, the relative likelihood is the relevant information. In a quantitative risk analysis, it is interesting to transform the likeliness into an expectation to occur over a period; a typical period is one year (for yearly estimations), and the usual figure is the ARO (Annual Rate of Occurrence). [...]*".

Likelihood can be expressed in different ways in Pilar, but basically we have five values[15]: VL, L, M, H, VH. Therefore, we are unaware about the numerical value that Pilar assigns to likelihood and, consequently, the simple equation $R = I \times L$ cannot be employed.

[15]These values were illustrated in Sec.3.1.1 as well.

In order to understand how risk is calculated by the tool, somehow we tried to reverse engineering the formula. Differently from the impact calculation, where we had the level map as cornerstone, here the process is entirely based on experiments and empirical data. Therefore, we created a simple project in Pilar with three assets and assigned only the indispensable values, bypassing aggravating/mitigating conditions as well as assets dependencies. Then we concentrated our analysis on a software assets for the availability security dimension.

Since risk is said to depend on two mainly factors, we started to observe its change in value by assigning different values to the likelihood, by holding the impact first, and to the impact, by holding the likelihood successively. As a result, we have conjectured a formula which seems to well approximate the values[16] returned as output by the tool:

$$R = 0.6I + L \tag{17}$$

where R is the risk, I is the impact and L is the likelihood value according to the following map: $VL \approx -0.9$, $L \approx 0$, $M \approx 0.9$, $H \approx 1.8$, $VH \approx 2.7$.

Proceeding in order, we observed that the risk value changes by a *delta* (or difference) of 0.9 when varying the likelihood by one step. This clarifies the reason why we assigned the foreseen values to the likelihood. Furthermore, taking this fact into account, we realised that the risk values can be approximated by Eq.17, as a result of further evidence empirically. In addiction, we can glance at the risk map derived from the conjectured formula in Fig.12, where we set the negative values to 0, because as we have already stated risk values range in $[0,9]$ in Pilar.

At this point, we decided to compare the values calculated by the conjectured formula with those returned in output by Pilar by performing a linear

[16] Later we will clarify that this conjecture works with outputs greater than or equal to 2, and why it happens as well.

0.6 I + L

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

Figure 12: Conjectured Risk Map

regression analysis, with a sample of 59 elements that should cover almost all possible outputs. The foreseen elements represent potential risk values and are taken from both the simple project and the case study project — the latter will be discussed in Sec.7.4.

It is important to highlight that regression analysis requires all items to be sorted in ascending (or descending) order, based on, in this case, one of the two columns. Thus, let the column of the risk values returned by Pilar (named PILAR) represent the independent variables, whilst let the column of the values calculated by using the conjectured formula (named Conjectured) be the dependent variables. Firstly, we are interested in how the two sets of values are related and, subsequently, we want to retrieve a linear regression equation to compare the trends. We can observe these risk values in Tab.5, already sorted by column "PILAR".

Conjectured	PILAR
0.9	0.4
1.8	0.57
0.9	0.75
-0.3	0.75
0.9	0.78
0	0.82
0.3	0.87
0	0.93
0.6	0.93
0.9	0.98
0.9	1
1.2	1.2
1.8	1.2
0.9	1.3
1.5	1.5
2.7	1.6
0.9	1.7
1.6	1.7
1.8	1.8
2.1	2.1
2.1	2.2
2.4	2.4
2.7	2.7

3	3
3	3.1
3.3	3.3
3.6	3.6
3.9	3.9
4.2	4.2
4.2	4.3
4.2	4.4
4.2	4.5
4.5	4.5
4.5	4.6
4.8	4.7
4.8	4.8
5.1	5.1
5.7	5.7
6	5.9
6	6
6.3	6.3
6.3	6.4
6.6	6.6
6.9	6.8
6.9	6.9
7.2	7.1
7.2	7.2

7.2	7.3
7.8	7.4
7.5	7.5
7.8	7.7
7.5	7.8
7.8	7.8
7.8	7.9
8.1	8
8.1	8.1
8.1	8.2
8.7	8.7

Table 5: Conjectured vs. PILAR Risk

Once we had the two sets to compare, we could proceed to perform a linear fit with the help of a tool, id est Google Sheets[17]. Particularly thanks to the help of the *CORREL* function, we found the following Pearson's r[18] (or Pearson correlation coefficient): $r = 0.9909792073$. Thereby, the two sets are strictly in a positive linear correlation. At this point, we calculated a linear fit with the help of the *LINEST* function, which returned the values of the intercept and the slope. Definitively, we have the following equation:

$$y = 0.97x + 0.15 \tag{18}$$

The comparison between the two sets is depicted by Fig.13 and Fig.14.

[17]Equivalent softwares can be used to perform regression analyses, such as Microsoft Excel, WolframAlpha, etc.

[18]A value of $+1$ is total positive linear correlation, 0 is no linear correlation, and -1 is total negative linear correlation.

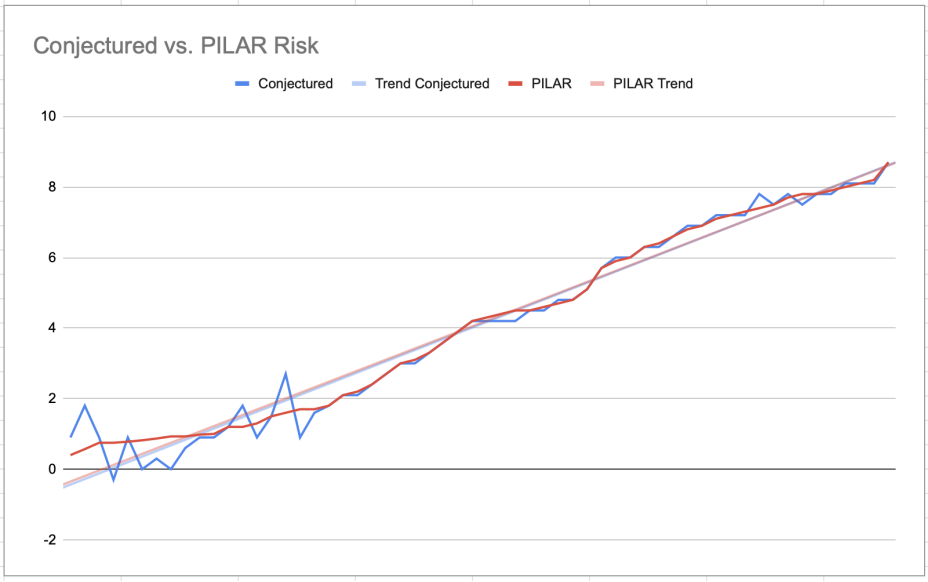


Figure 13: PILAR Risk Linear Regression

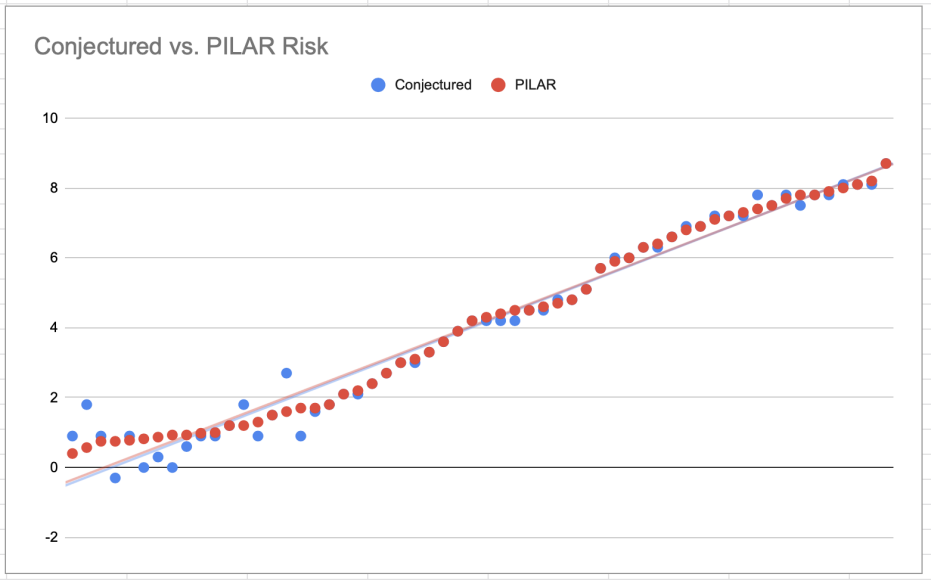


Figure 14: PILAR Risk Linear Regression

In the ordinate axis we have the value of the risk — remember that this range is between 0 and 9 in Pilar. As we can notice, the two sets actually follow the same trend. Especially, the points are strictly close each other starting from a risk value of 2. If we observe the red line (PILAR) in Fig.13, it is undeniable that the formula used by Pilar assumes a different behavior near the lower values. On the other hand, the conjectured formula can assume negative values, which clashes with the domain of the risk values. However for risk values above this threshold, the conjectured formula expressed in Eq.17 empirically seems to fit the actual values as well.

Before concluding this chapter it is also important to highlght that, while performing these kind of experiments, we noticed the risk values calculated by the tool vary — albeit by a few decimals — depending on the type of threat considered. This might be due to what the documentation defines as the "*relative likelihood*" of a threat and, logically, it might also be related to the class which the asset belongs to, as well.

Eventually, despite Pilar does not officially provides a clear equation for risk calculations, we identified a possible trend of the data and gave an empirical formula which works for potential risk values greater than or equal to 2.

7 Case Study Report

In this case study we consider a standard structure which a classical automotive company may assume, also inspired by the Toyota Motor Corporation automotive system[36] — particularly for car components and other services infrastructures. The risk assessment process mainly focuses on the smart car product. The company is composed of the most common departments for this kind of business. Among others, we recall Production/Manufacturing, Maintenance and Utilities, IT, Research & Development, Supply Chain and Logistics, Sales & Marketing and Finance & Cost Control. It is necessarily to highlight that most of the company departments are ignored, because they are not strictly related to the main character of the analysis, the car product as we previously stated. Since smart cars are supposed to be connected to both other internal and external services, we also add some boundaries components to this case study, such as Smart Traffic Monitoring and Insurance Company.

Below an outline of automotive security risks is provided, followed by a description of the automotive system considered as our case study scenario. Note that these sections introduce a risk assessment process. According to the guidelines expressed in Magerit, the process starts with a threat modeling process[19] and keeps on a demo by using the PILAR software.

[19]The STRIDE methodology is chosen for this purpose. It was introduced in Sec.4.1

7.1 Automotive Security

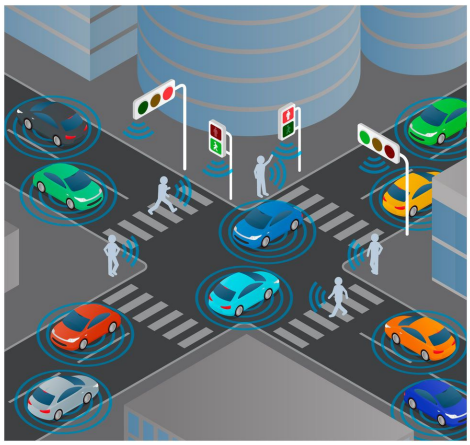


Figure 15: Vehicle-to-Everything

Nowadays vehicles are more electronic than ever. Actually as of 2009, vehicles have typically been built with over 100 micro processors, 50 electronic control units, 5 miles of wiring, and 100 million lines of code[11], as reported in IEEE Spectrum by an article titled "*This Car Runs on Code*". Even engineers at Toyota joke that the only reason they put wheels on a vehicle is "to keep the computer from scraping the ground". Moreover, vehicle automation has been one of the fundamental applications within the field of intelligent transportation systems (ITS) since the start of ITS research in the mid-1980s[12].

Over the last few years, terms like "self-driving" cars and "connected vehicles" are increasingly common. In particular, the latter refer to the **Vehicle-to-everything (V2X)** paradigm[29][30], that is communication between a vehicle and any entity that interact within the vehicle. More in detail, behind the term "connected vehicles" we can identify more specific types of communication: *V2I (vehicle-to-infrastructure), V2N (vehicle-to-network), V2V (vehicle-to-vehicle), V2P (vehicle-to-pedestrian), V2D (vehicle-to-device)* and *V2G (vehicle-to-grid)*.

As computer systems become more integral to vehicles, performing security reviews becomes more important and complex. The term "**Automotive Security**[20]" refers to a branch of cybersecurity dedicated to the threats associated with vehicles[31]. The ECUs (Electronic Control Units) represent an example of the most relevant components implemented inside vehicles. These units nowadays control almost everything in the vehicle, from simple tasks such as activating the wipers to more safety-related ones like brake-by-wire or ABS (Anti-lock Braking System). Autonomous driving is also strongly reliant on the implementation of new, complex ECUs such as the ADAS, alongside sensors (lidars and radars) and their control units. Inside the vehicle, the ECUs are connected with each other through cabled or wireless communication networks, such as CAN bus (Controller Area Network), MOST bus (Media Oriented System Transport), FlexRay or RF (Radio Frequency) as in many implementations of TPMSs (Tire Pressure Monitoring Systems). It is important to notice that many of these ECUs require data received through these networks that arrive from various sensors to operate and use such data to modify the behavior of the vehicle (e.g., the cruise control modifies the vehicle's speed depending on signals arriving from a button usually located on the steering wheel).

Since the development of cheap wireless communication technologies such as Bluetooth, LTE, Wi-Fi, RFID and similar, automotive producers and OEMs have designed ECUs that implement such technologies with the goal of improving the experience of the driver and passengers. Also, the rise of Internet of Things (IoT) "smart devices" contributes substantially both to previously unthinkable useful features, and to the exposure of threats — since the attack surface is more extensive. Safety-related systems such as the OnStar from General Motors, telematic units, communication between smartphones and the vehicle's speakers through Bluetooth, Android Auto and Apple CarPlay, and RKES (Remote Keyless Entry Systems) are just ex-

[20]Not to be confused with automotive safety.

amples of how the vehicle has become externally connected to devices and, in some cases, to the Internet.

Although on the one hand the implementation of new technologies — semi-autonomous and autonomous cars which make use of advanced Machine Learning (ML) and Artificial Intelligence (AI) techniques are emerging as well as 5G connectivity enforcement — improved the safety and driving experience of the vehicle, on the other hand the increasingly high number of externally-communicating units has led to an increment in the dimension of the attack surfaces of each vehicle. There are many examples of car hacking in literature — most of them were presented at the Black Hat security conferences — where electronic control units have been exploited as attack vector, due to their capability of modifying the behavior of the vehicle. Therefore, it is necessary to ensure that an attacker cannot have the chances to take control of critical systems inside the vehicle. Fortunately, in the latest years, the new concept of automotive security started to become more and more important when designing new vehicles. Among others, the in-vehicle infotainment (IVI) system is also to be considered a critical point, as well as the CAN Bus.

Just to mention a couple of examples, we recall that researchers discovered 19 security flaws in Mercedes-Benz vehicles and disclosed them at Black Hat USA 2020[32]: "*[...] By exploiting these vulnerabilities, we can remotely unlock the door and start the engine and they potentially impact all Mercedes-Benz connected cars in China (estimated over 2 million)*". Other two researchers presented at Black Hat USA 2015 how they had tried to hack the multimedia system of Jeep through Wi-Fi connection[33]. It turned out that was easy "*to hack it due to the fact that the WiFi password is generated automatically, based on the time when the car and it's multimedia system is turned on for the very first time*". As an icing on the cake, the year later, the so called "Jeep hackers" presented more dangerous vulner-

abilities at Black Hat USA 2016. Last but not least, at STRIVE 2019 researchers presented CANDY CREAM[34]: "*an exploit that works on an Android In-Vehicle Infotainment (IVI) system connected to the CAN bus of a car*". CANDY CREAM exploits a found vulnerability to remotely access the Android infotainment system, then the exploit injects in the Infotainment system to attack the instrument cluster of the car. Particularly, it is able to send random CAN data frames to activate the odometer, show the alert indicators, show the lights indicators.

Generally, attacks targeting smart cars may lead to vehicle immobilisation, road accidents, financial losses, disclosure of sensitive and/or personal data, and even endanger road users' safety. Moreover in order to conclude the overview about automotive security, we classify breaches in the security of vehicles from a stakeholders point of view:[35]:

- *Privacy* - unwanted or unauthorised acquisition of data relating to vehicle/driver activity, vehicle/driver identity data, or vehicle/sub-system design and implementation.
- *Financial* - unwanted or unauthorised commercial transactions.
- *Operational* - unwanted or unauthorised interference with on-board vehicle systems or V2X communications that may impact on the operational performance of vehicles and/or intelligent transportation systems (ITS) (without affecting physical safety).
- *Safety* - unwanted or unauthorised interference with on-board vehicle systems or V2X communications that may impact on the safe operation of vehicles and/or ITS.

7.2 Automotive System Description

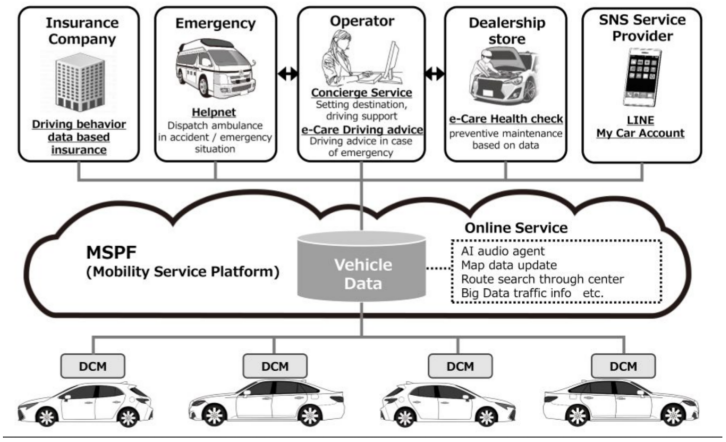


Figure 16: Toyota Automotive System

In this section we present the leading parts of the automotive system that are relevant to the risk assessment process.

7.2.1 Car Description

The car product comes standard with an on-board *Data Communication Module (DCM)* that links to a *Controller Area Network (CAN)*. By using this hardware, the car is connected to several services through the *Mobility Service Platform (MSP)*, an information infrastructure developed by the company for connected cars. Moving forward, the company aims to equip most new passenger vehicles in its domestic market with DCM. Cars are also equipped with an *Automotive Head Unit* that interacts with other components, such as *Multimedia Playback, Applications*, long and short rage communication protocols, i.e., *Bluetooth, WiFi, 3G/4G/5G, DSRC/WAVE, GPS*. The company considers some connected services essential for drivers to safely, intuitively and effortlessly enjoy their cars. Connected cars, linked to the MSP, offer customers ways to better understand, use, and care for their vehicles.

7.2.2 Company Services Description

Operator-based services offer drivers two main benefits. The first consists of an operator made available to set the destination of the on-board navigation system. The second concerns driving support, offering advice to drivers by diagnosing technical faults based on the data of the connected vehicles. This advantage comes from a feature called "e-Care Driving Guidance", where a remote operator is able to speak directly to the driver through the on-board microphone and speaker in the event of a technical failure. The operator can review the vehicle data provided by the DCM and provide troubleshooting procedures or advise the driver to take their vehicle to their usual or nearest service dealer. For example, the auxiliary battery starting voltage of any vehicle gradually decreases over time. With the data provided, an alarm will be shown on the dealership's operating platform and the dealership staff will contact the driver and recommend a battery replacement before the customer has trouble starting the vehicle. The dealership's message is sent to the car's navigation unit and read aloud to the driver.

Customers can also use a smartphone application connected to their car. Drivers will be able to interact with the vehicle for different purposes. For example, you can use the app to open/close car doors or to enter a destination that will be sent to the in-vehicle navigation system. The app can also provide information such as the ideal departure time, empty distance and fuel efficiency, based on time and distance to the destination, but also the state of wear of the car's components, and so forth.

The company offers an "Emergency Helpnet" service linked to both a sensor in the airbags and the driver's application. Upon detecting the alarm activation, a service operator will immediately review the data sent by the DCM and attempt to contact the customer to assess the situation. Depending on the customer's response, or lack thereof, the operator is then able to alert the fire brigade or ambulance services. If the emergency services deem seri-

ous injury likely, they can respond, possibly including by sending a medical helicopter or similar together with a doctor to provide emergency medical care. This service covers the entire country where the company is based.

The standardisation of DCM also makes it possible to introduce automobile insurance based on actual driving behavior data. Drivers will be assigned a safety score based on the driving data collected in the MSP. Drivers can use their smartphone to check their safe driving scores. This score can then be part of a new data-driven insurance, called the "Connected Car Insurance Plan". The insurance premium will be updated monthly based on the policyholder safe driving score and distance traveled and notifications sent to the customer via their smartphone.

Using voice recognition, an Artificial Intelligence (AI) virtual agent can be accessed using the natural language of the driver or passenger to be able to set the destination for the navigation system, manage the audio system or even provide instructions to use the car equipment. The AI is designed to understand even complicated requests such as "Search for restaurants around here, preferably with a parking space" and is linked to the smartphone application.

Eventually, thanks to the cloud and big data, the onboard navigation system will always have access to the latest version of the program and map data. To provide customers with real-time services, the navigation system will use maps and real-time traffic data to suggest optimal route information to help drivers reach their destination, automatically switching from the cloud to the on-board computer for optimal calculations route and position searches.

7.3 Threat Modeling

In Sec.4.1 we outlined the STRIDE methodology for threat modeling. This approach is compliant to the Magerit guidelines, thereby we can use this methodology in order to identity assets, threat agents and the potential threats which may afflict the company and, more broadly, the entire automotive system.

The following sections are indeed planned to describe these steps. It is important to highlight that the latter are preparatory to the PILAR demo proposed in Sec.7.4, since they simply the forthcoming work for a cross-analysis between our "by-hand" identified resources and those proposed automatically by the tool.

7.3.1 Assumptions

Assumptions help to understand some critical behaviours behind the scenes. For simplicity, we assume that the Company security domain can be considered as nearly "safe" from known tech-related threats, thereby the core of the analysis will focus on the Car security domain as well as the Base domain for customers' data. For obvious reasons, external services are assumed to be safe as well.

Therefore, in Tab.6 a list of assumptions is illustrated to better justify the threats identification process, described in Sec.7.3.4. Moreover, note that most of the following assumptions are consequence of the structure of the automotive system which we previously described in Sec.7.2 and it summarise the most relevant concepts.

Assumption Notes	
ID	Description
AN1	*Assumptions related to Company Domain*
AN1.1	The Internal Services network is fragmented to multiple LANs (separation of duties enforcement).
AN1.2	The Internal Services network used by employees is only accessible through a dedicated VPN.
AN1.3	In Internal Services all the network traffic is encrypted using the TLS 1.1 protocol.
AN1.4	In Internal Services a log system is used to traceback critical events performed by employees.
AN1.5	In Internal Services an NGINX Web server (A1.1) is used to interact within an internal Oracle MySQL database (A1.2).
AN1.6	In Internal Services employees are equipped with company devices (A1.6). The latter have different features depending on the personnel's tasks.
AN1.7	In Dealership Store & Help Center all the network traffic is encrypted using the TLS 1.3 protocol.
AN1.8	In Dealership Store & Help Center an NGINX Web server (A1.3) is used to interact within an internal Oracle MySQL database (A1.4).
AN1.9	In Emergency Helpnet all the network traffic is encrypted using the TLS 1.3 protocol.
AN1.10	In Emergency Helpnet an NGINX Web server (A1.3) is used to interact within an internal Oracle MySQL database (A1.4).
AN1.11	In Dealership Store & Help Center there is no separation of duties. An employee can act as an administrator as well as an ordinary user.
AN1.12	The Customers' Mobile Application provides a front-end to communicate within the Dealership Store & Help Center (A1.3) and Emergency Helpnet Web (A1.5) servers.

AN1.13	In the Customers' Mobile Application a user authenticates themselves by providing a UID and a password (A1.5). The password must be at least 6 characters long (numbers, special characters or capital letters are not necessarily required). Multi-factor authentication (MFA) is not adopted.
AN1.14	The Emergency Helpnet is an internal service offering support to users via the Customers' Mobile Application.
AN1.15	The Smart Traffic Monitoring is an external service interacting with Mobility Service Platform (A2.3), where data is sent from the Data Communication Module (A2.2) of a car product.
AN1.16	The Insurance Company is an external service interacting with the Mobility Service Platform (A2.3).
AN2	*Assumptions related to Car Domain*
AN2.1	The Data Communication Module (A2.2) provides exchange of information data between the car product and the Mobility Service Platform (A2.3).
AN2.2	In the Data Communication Module (A2.2) information is not anonymised and data is sent unencrypted to the Mobility Service Platform (A2.3).
AN2.3	The Automotive Head Unit (A2.4) firmware is Android based.
AN2.4	In the Automotive Head Unit (A2.4) no login credentials are required by default to perform any operation. A password can be set by the customer without any strength limitations.
AN2.5	The Bluetooth module (A2.6) is used to lock/unlock the car product via a Customers' Mobile Application feature.

Table 6: Assumed facts

7.3.2 Assets Identification

An asset is a component or function of an information system that may be subject to deliberate or accidental attacks that may have consequences for the organisation[21]. Assets include: information, data, services, applications (software), equipment (hardware), communications, media, facilities, and personnel. In other words, an **asset** is anything that has business value and that must be protected from misuse by adversaries. The business value of an asset can range from very high to very low. Particularly relevant are the *essential assets*, which represent the requirements of the risk owners: the security requirements. Basing on Magerit, in our case study we identify two essential assets: the information that is handled, i.e., customers' data[21], and the services which are directly provided by the company, such as DSHC, EH and MSP[22] services.

In general, assets are organised into trees or graphs showing dependencies, where the security of the assets higher up in the tree depends on assets in the lower positions. When we move top-down, we talk about dependencies: upper assets depend on lower assets to protect their security requirements. And the other way round, when we move bottom-up, incidents on lower assets have an impact on the upper ones. The value of an identified assets is defined as the security properties — this concept will be recalled in the Threats Identification section — to be protected. There are three conventional security properties known as **CIA triad** (*confidentiality*, *integrity* and *authentication*). Other security properties which should be taken into account are *authorisation* and *accountability*.

In Tab.7 a comprehensive list of the identified assets is shown.

[21] Information linked to a customer handled by both internal and external services.

[22] The Mobility Service Platform is particularly related to the Smart Traffic Monitoring service, and others V2X peers.

Assets		
ID	Security Domain, Asset Name	Description
A0	Base	*Assets related to Base Domain*
A0.1	Customer data	All the customer's data handled/gathered by the Car/Company components.
A1	Company	*Assets related to Company Domain*
A1.1	IS Web server	The Internal Services Web server used to interact with the Internal Services database (A1.2).
A1.2	IS database	The Internal Services database storing information for the IS Web server (A1.1).
A1.3	DSHC Web server	The Dealership Store & Help Center Web server used to interact with the DS&HC database (A1.4). It also communicates with the Customer's Mobile Application.
A1.4	DSHC database	The Dealership Store & Help Center database storing information for the DS&HC Web server (A1.3).
A1.5	EH Web server	The Emergency Helpnet Web server used to interact with the EH database (A1.6). It also communicates with the Customer's Mobile Application.
A1.6	EH database	The Emergency Helpnet database storing information for the EH Web server (A1.5).
A1.7	CMA authentication credentials	Username and password for the Customers' Mobile Application access.
A1.8	Personnel's devices	Physical devices used for personnel' tasks.
A2	Car	*Assets related to Car Domain*
A2.1	CAN Bus	The CAN Bus is a robust vehicle bus standard used for internal communication messages between ECU components.

A2.2	DCM	The Data Communication Module is used to communicate information (i.e., traffic analytics for the Smart Traffic Monitoring service and/or Insurance Company, the detection of a car burglar intrusion, etc.) to the MSP (A2.3).
A2.3	MSP	The Mobility Service Platform provides a cloud system to share driving-related data coming from the DCM (A2.2) with both internal and external services (e.g., Emergency Helpnet, Smart Traffic Monitoring, Insurance Company).
A2.4	Automotive Head Unit	The Automotive Head Unit provides a unified hardware interface for the system, including screens, buttons and system controls for numerous integrated information and entertainment functions.
A2.5	GPS	The GPS module used for transmitting the car position information.
A2.6	Bluetooth	The Bluetooth 5.0 module used to interact within the IVI system as well as to unlock the car by using a smartphone.
A2.7	WiFi	The WiFi IEEE 802.11 module used to connect to a WiFi network.
A2.8	4G/5G	The 4G/5G module used to connect to the Internet.
A2.9	DSRC/WAVE	The Dedicated Short Range Communications/Wireless Access in Vehicular Environments modules used to connect IoT devices and components in the IVI system (A2.4).
A2.10	USB	The USB input port.
A2.11	Multimedia Playback	The Multimedia Playback is a component used for in-car entertainment.
A2.12	Applications	The applications installed in the Automotive Head Unit (A2.4) OS.

Table 7: Identified assets and their descriptions

7.3.3 Trust Levels for Threat Agents

Trust levels represent the access rights granted to entities (human users, devices and services) and enforced by the system. Generally, threats can originate from two primary sources: internal agents (someone with authorised access) and/or external agents (someone with unauthorised access). A **threat agent** is an individual or group that can manifest a threat. It is fundamental to identify who would want to exploit the assets of a company, and how they might use them against the latter.

In our case study classification, we identify Customer (TA1) and Adversary (TA4) as external threat agents, and Personnel (TA2) and Administrator (TA3) as insider threat agents:

- *Customer (TA1)* - have access to their own car, Customers' Mobile Application and personal records. Generally, customers have enough resources to attack a system, but those who are not IT experts have low skills to perform such malicious actions. Customers may act with either good or evil intentions to gain privileges not generally assigned to them.

- *Personnel (TA2)* - have access to their own devices to fulfil their tasks, such as sell a car product, offer assistance to customers, and other Internal Service assignments. Personnel may also have adequate resources to attack a system because they have access to it, but their attack skills may be low since in most company departments they are unlikely to be IT experts.

- *Administrator (TA3)* - are responsible for system operation and/or maintenance. It is assumed that a system administrator has access to all system components, in order to ensure the correct operation of hardware and software. However, they should not have access to any car-related information of the customers. Administrators have suffi-

cient resources and high IT skills. On the one hand, administrators are generally very trustworthy, but some of them who are not well-trained might unintentionally threaten the system. On the other hand, administrators who are dissatisfied or have been bribed may become spiteful and intentionally cause harm to the system.

- *Adversary (TA4)* - have malicious or fraudulent intentions to intentionally threaten the system. Adversaries can be categorised as car thieves or attackers who try to get profit by compromising the system. Generally, they are medium/high IT skilled, thereby adversaries should not be underestimated.

The foreseen entities are summarised in Tab.8, including their variations.

Threat Agents		
ID	Name	Description
TA1	Customer	
TA1.1	Customer with valid credentials	A user who uses CMA authentication credentials (A1.5) to log in.
TA1.2	Customer with invalid credentials	A user without CMA authentication credentials (A1.5) who attempts to log in using invalid credentials.
TA2	Personnel	
TA2.1	Personnel with valid credentials	A user who legitimately logs into the IS Web server (A1.1).
TA2.2	Personnel with invalid credentials	A user who attemps to log into the IS Web server (A1.1) using invalid credentials.
TA3	Administrator	
TA3.1	IS server admin	The database server administrator has read and writes access to the database (A1.2).
TA3.2	DSHC server admin	The database server administrator has read and writes access to the database (A1.4).
TA4	Adversary	
TA4.1	Car thief	A user who attempts to steal the car product.
TA4.2	Attacker	A user who attempts to sabotage the automotive system for profit.

Table 8: Identified threat agents

7.3.4 Threats Identification

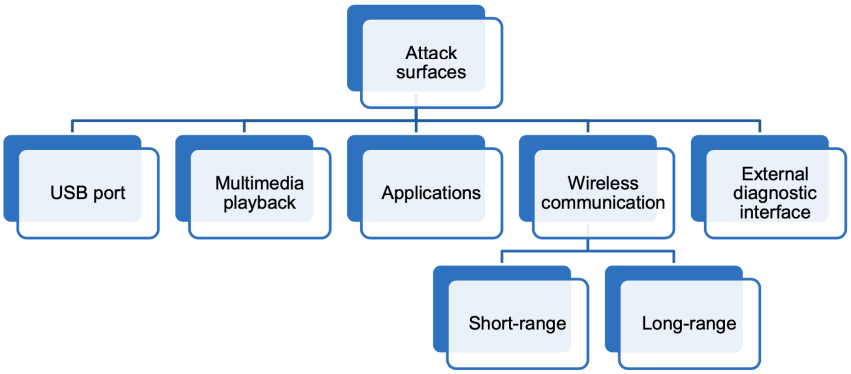


Figure 17: Attack Surface in IVI System

We categorise threats according to the following types (or classes): Authentication, Authorisation and Access Control, Availability, Confidentiality and Privacy, Auditing and Logging. Threats in an automotive system, as we outlined in Sec.7.1 are based on both real-world and theoretically possible attacks. Most real-world attacks aim at the safety of the people in and around the car, by modifying the cyber-physical capabilities of the vehicle (e.g., steering, braking, accelerating without requiring actions from the driver), while theoretical attacks are supposed to focus also on privacy-related goals, such as obtaining GPS data on the vehicle, or capturing microphone signals and similar. Before continuing the threats identification process, it is important to highlight that, most of the IVI system threats analysed below refer to the Common Attacks Against Car Infotainment Systems[38], which were introduced at the Automotive Linux Summit 2019.

In general threats involve potential damage, which is classified as very low, low, medium, high or very high, according to the distribution of the business functions and processes. For instance, if one customer's login credentials were lost (or stolen), the impact would be low, because the damage would

only affect one user; but if a personnel's identity was stolen, the impact would be very high, because this may affect more than one customers.

It is important to note that in the proposed analysis we intentionally omitted threats of natural and industrial origin as they will be automatically considered[23] in Sec.7.4 by the tool itself. Below we provide a brief description of the identified threats. These are summarised in Tab.9, including their related STRIDE rate and a first estimate of the impact values as well as the involved threat agents.

In **Authentication Threat Class (T1)** all possible threats related to user's identity and login credentials — possibly enabling others to gain access to the system on "behalf of" the user — are defined. The main concerns are loss (or theft) or sharing of users' identities and login credentials. Users sharing their login credentials with friends, relatives and/or other users may cause potential impact, like identity misuse, tampering with customer data, or private information disclosure, among others. Moreover, Customers' Mobile Application authentication credentials are very important, since they allows the user to authenticate with the DSHC/EH servers and other services. Speaking of which, we remember that the customer's identity is also important for benefits such as insurance points, thereby the user's identity and login credentials have to be protected as well. It is also important to highlight that communication modules represent a critical point for authentication threats. Adversaries might indeed spoof the customer's identity by exploiting COM modules. Moreover, if any third-party services use the customer GPS location for the user authentication, the exploitation of the GPS module could represent a threat for the customer. The same considerations can be made for the other communication modules, although paying attention that, in the case of the DSRC/WAVE module for example, it is not the

[23] Afterwards we will perform a cross-analysis between the threats here identified and those proposed automatically by Pilar.

customer's identity that is spoofed but that of the car as a node in the network. It is natural that a spoofing attack, or an identity theft, to personnel and/or system admins could led to high severity impact, as customers and personnel data could potentially be disclosed or modified. Therefore, for both customers and personnel, we ought to take into consideration social engineering attacks, which may led to spoofing identity as well as information disclosure.

In the second category, **authorisation and Access Control Threat Class (T2)**, threats include elevation of privilege, data tampering and/or disclosure of confidential data. We ought to consider that elevation of privilege threats may let insiders attempt to gain additional access to system components. For example, personnel may impersonate the context of administrators — by exploiting some weakness in the access control protocol — in order to gain additional privileges and more control over the system or access to a specific resource in a fraudulent manner. These could be confidential data, such as customers' records, which thus can be viewed by unauthorised users due to improper data protection. In this threat class, the majority of threats are high rated, because for instance, gaining access to powerful accounts — such as those of members of local administrator groups or local system accounts — may cause massive damage to customers or company departments. Furthermore in some of the car communication modules, such as the DCM, data is not encrypted and there is no access control to data circulating on the network. This may obviously lead to information disclosure threats. Speaking of authorisation, it is important to emphasise that the Automotive Head Unit could be a single point of entrance to multiple exploits, as it is linked to several infotainment components (i.e., COM modules, multimedia, applications, etc.). For instance, a maliciously crafted USB device within a modified firmware inserted by the user (social engineering), could led to persistent root code execution for adversaries, i.e., by exploiting a vulnerability in the update mechanism. This would allow malicious users to

leverages SMS service on the paired driver's phone to access personal information, intercept banking authentication pins, or even block phone calls. They could also command the IVI system remotely through SMS messages. In other cases, specially prepared media files might led to information disclosure (and privilege escalation), as a song could alter the firmware of the car's stereo system, giving adversaries an entry point to change other components on the car. Last but not least, applications installed in the Automotive Head Unit may represent a gold mine for adversaries, as they could exploit any vulnerability, e.g., the browser rendering process, to gain code execution on the car's firmware.

For **Availability Threat Class (T3)** threats, we have to take into account the importance of the main services. The company should ensure that significant elements, such as servers and car components (e.g., communication modules, IVI system, etc.), can be susceptible to denial of service threats. These may often arise from both insiders or external agents, because of intentional or unintentional actions. While on the one hand a denial of service to IS (or other departments) would result in purely economic losses for the company, on the other hand an attack of this type aimed at targeting the emergency service (DSHC) for the customer, would result in more significant damage. Speaking of customer's health, availability threats which involve car components must be considered very dangerous. This can be especially the case of DoS attacks to the ECU (electronic control unit), triggering possible serious consequences for the driver's physical health, indeed. Furthermore, we should take into account that adversaries may deny access to the MSP to take advantage of that (i.e., a car thief makes him lose track by cutting the car off the net) or just to cause damage to the automotive system (e.g., jamming attacks such as black hole). In the latter scenario, we can also include a DoS attack to stop, for instance, a moving car by exploiting COM modules, such as Bluetooth — gaining the ability to lock/unlock the car as well as perform an OBD II dongle attack. In this threat class, it is

also important to include natural threats arising from natural disasters, such as earthquakes, volcanic eruptions, tsunamis, fires and floods. Note that we omit the threat agents in this case for obviously reasons.

In the fourth section of the table, threats are related to **Confidentiality and Privacy Threat Class (T4)**. Privacy is subject to a variety of threats, including access to sensitive data in storage and data tampering. Threats to sensitive data in storage can affect data stored in the IS/DSHC/EH servers. Improper data protection, on both company services and car components, may allow attackers to read information not intended for disclosure. For this purpose, it is essential to specify that — as we previously stated for Authentication (T1) threats — social engineering may led to malicious information disclosure. The unconscious use of malware or file-sharing tools could also result in high severity consequences for sensitive data. Moreover, particular attention should be paid to the MSP, which represents a critical asset due to the huge flow of information circulating in it. An unauthorised disclosure to the MSP might result in a very high impact for the huge amount of users involved. Last but not least, we also ought to consider some IVI components dealing with personal data. For instance, the Automotive Head Unit is a critical point for personal customers' information as it deals with all the entertainment features. Adversaries who have access to it may, for instance, leverage SMS service on the paired driver's phone to access personal information, intercept banking authentication pins, or even block phone calls. Also, GPS and Bluetooth modules can represent a gold mine for adversaries who want to track customers' locations as well as access user's stored data (e.g., contacts, call logs, text logs, etc.). Before proceeding, it should be pointed out that an unauthorised disclosure would not only affect the customers concerned, but also economic damage to the company resulting from any legal sanctions in the event that there is no compliance with regulations for the protection of personal data, such as GDPR.

In the final section, threats related to **Auditing and Logging (T5)** are listed. Generally, auditing and logging should be used to help detecting suspicious activities, such as footprinting or possible password cracking attempts before exploitation actually occurs. These can also help dealing with the threat of repudiation. It is much harder for a user to deny performing an operation if a series of synchronised log entries on multiple servers indicate that the user indeed performed the transaction. Threats related to auditing and logging include potential data repudiation, log tampering and insufficient auditing. For example, a customer or personnel denies or claims that they did not receive, write or edit data. Log tampering entails an insider attacking logs via log files. For threats due to insufficient auditing, the logs must capture enough data to display what happened in the past and they must be well-protected to ensure that attackers are not able to cover their tracks. Impacts to these kind of threats is high when the threat agents are personnel/admins or adversaries.

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
T1.3	**Identity spoofing**: customers or personnel reveal login credentials to someone (e.g., social engineering attack).	TA1.1, TA2.1	S	Medium
T1.4	**Identity theft and misuse**: customers act "on behalf of" the user to take advantage of their identity-related benefits (e.g., EH services, insurance points) by viewing or tampering with DCM packets from the user's car.	TA1.1	S	High

T1.5	**Identity theft and misuse**: system admins misuse customers identity for malicious acts (e.g., curiosity, disclosure, fraud and/or sabotage).	TA3.1, TA3.2	S	High
T1.6	**CAN packets tampering**: customers or car thieves view CAN packets and learn the behavior of the other nodes of the network, so that they falsify data, send messages pretending to be another node of the network (e.g., replay or masquerade attacks).	TA1.1, TA4.1	T	High
T1.7	**COM packets spoofing**: adversaries or car thieves view communication protocols' packets and learn how to reply to them so that they can act "on behalf of" the user. This might involve the Bluetooth, GPS, WiFi, 3G/4G/5G and DSRC/WAVE modules by performing different types of attacks (i.e., MitM, replay, etc.).	TA4.1, TA4.2	S	High
Threats Class 2 (T2): Authorisation and Access Control				
ID	Description	TA	STRIDE	Impact

T2.1	**Unauthorised access**: unauthorised access to system data using shared (or stolen) passwords.	TA1.1, TA2.1, TA4.1, TA4.2	E	High
T2.2	**Unauthorised access**: system admins and personnel gain intentional unauthorised access to customer data for malicious acts (e.g., curiosity, disclosure).	TA2.1, TA3.1, TA3.2	E	High
T2.3	**Data tampering**: customers intentionally or accidentally modify, add and/or delete data because of over-privileges or inapplicable access control of a resource.	TA1.1	T	Medium
T2.4	**Data tampering**: personnel and system admins intentionally or accidentally modify, add and/or delete data because of over-privileges or inapplicable access control of a resource.	TA2.1, TA3.1, TA3.2	T	High
T2.5	**Elevation using impersonation**: personnel or system admins may impersonate the context of other personnel or system admins in order to gain additional privileges.	TA2.1, TA3.1, TA3.2	E	High

T2.6	**Unauthorised access to administration interfaces**: malicious users may be able to gain access to configuration management through administration interfaces.	TA1.1, TA2.1, TA4.2	E	High
T2.7	**Weak access control**: improperly separation of duties can led personnel and system admins intentionally or accidentally read information not intended for disclosure.	TA2.1, TA3.1, TA3.2	I	Medium
T2.8	**Unauthorised access**: adversaries take advantage of social engineering to make the user insert a maliciously crafted USB device, so that they can install a malicious firmware via USB and gain persistent root code execution.	TA1.1, TA4.1, TA4.2	E	Very High
T2.9	**Unauthorised access**: adversaries specially prepare media files to tamper with media engine services, Bluetooth and WiFi stacks. They add extra code to a digital music file to turn a song burned to CD into a Trojan horse.	TA1.1, TA4.1, TA4.2	I	High

T2.10	**Unauthorised access**: adversaries exploit a vulnerability in any application, i.e., the browser renderer process so that they execute code on the car's firmware.	TA1.1, TA4.1, TA4.2	E	High
T2.11	**Lack of access control**: adversaries access to information not intended for disclosure by viewing unencrypted packets from the DCM.	TA4.1, TA4.2	I	High
Threats Class 3 (T3): Availability				
ID	Description	TA	STRIDE	Impact
T3.1	**Denial of service**: adversaries deny access to the IS server by flooding it with TCP/IP packets.	TA4.2	D	Medium
T3.2	**Denial of service**: adversaries deny access to the DSHC server by flooding it with TCP/IP packets.	TA4.2	D	High
T3.3	**Denial of service**: adversaries deny access to the Emergency Helpnet server by flooding it with TCP/IP packets.	TA4.2	D	High
T3.4	**Denial of service**: adversaries deny access to the ECU by abusing the error handling protocol of CAN.	TA4.1, TA4.2	D	Very High

T3.5	**Denial of service**: adversaries deny access to the MSP by fuzzing and flooding it with malformed packets sent from the DCM.	TA4.1, TA4.2	D	High
T3.6	**Denial of service**: adversaries fuzz the firmware of the Automotive Head Unit denying its functionalities.	TA4.2	D	Medium
T3.7	**Denial of service**: car thieves view BT packets and gain the ability to lock/unlock the car, as well as perform an OBD II dongle attack.	TA4.1	D	High
T3.8	**Denial of service**: adversaries deny access to the WiFi related features by performing jamming signals at the physical layer, deauthing or flooding attacks.	TA4.1, TA4.2	D	High
T3.9	**Denial of service**: adversaries jam signals at the physical layer, denying access to the DSRC/WAVE component (black hole attack).	TA.4.2	D	High

T3.10	**Natural or industrial disaster**: disastrous events of natural or industrial origin (e.g., earthquakes, volcanic eruptions, tsunamis, fires, floods, etc.) deny access to the company services or the car functionalities.	N.A.	D	High
Threats Class 4 (T4): Confidentiality and Privacy				
ID	Description	TA	STRIDE	Impact
T4.1	**Unauthorised disclosure**: customers accidentally access some confidential data via malware or non-official Customers' Mobile App.	TA1.1	I	Low
T4.2	**Unauthorised disclosure**: personnel and system admins intentionally or accidentally access some confidential data via malware or file-sharing tools installed on their communication devices.	TA2.1, TA3.1, TA3.2	I	High
T4.3	**Lost device**: personnel losing their devices would cause exposure of sensitive data such as login credentials.	TA2.1	I	Medium
T4.4	**Stolen device**: theft of personnel devices that would cause exposure of sensitive data such as login credentials.	TA2.1	I	Medium

T4.5	**Unauthorised disclosure**: adversaries install some malware (or perform a social engineering attack) in the Automotive Head Unit and access some confidential data of the user.	TA1.1, TA4.1, TA4.2	I	Very High
T4.6	**Unauthorised disclosure**: customers or adversaries intentionally or accidentally access some confidential data of a user en route within the MSP.	TA1.1, TA4.1, TA4.2	I	Very High
T4.7	**Unauthorised disclosure**: adversaries intentionally access private user's information (e.g., microphone signals) by installing a malware in the Automotive Head Unit.	TA4.1, TA4.2	I	High
T4.8	**Unauthorised disclosure**: adversaries intentionally access user's GPS location information by sniffing GPS packets.	TA4.1, TA4.2	I	High

T4.9	**Unauthorised disclosure**: adversaries intentionally access user's stored contacts, call logs, text logs, and in some cases even full text messages without the vehicle's owner being aware, by performing a CarsBlues attack.	TA4.1, TA4.2	I	Very High
Threats Class 5 (T5): Auditing and Logging				
ID	Description	TA	STRIDE	Impact
T5.1	**Potential data repudiation**: customer denies or claims not receiving, writing or editing data.	TA1.1	R	Low
T5.2	**Potential data repudiation**: personnel or admins deny or claim not receiving, writing or editing data.	TA2.1, TA3.1, TA3.2	R	Medium
T5.3	**Log files tampering**: customers, adversaries, system admins or personnel delete or update log files in any way.	TA1.1, TA2.1, TA3.1, TA3.2, TA4.2	T	High
T5.4	**Insufficient auditing**: logging sufficient and appropriate data to handle repudiation claims.	TA1.1, TA2.1, TA3.1, TA3.2, TA4.2	R	High

Table 9: Identified threats

7.4 PILAR Demo

For our case study we created a project named "AURA01" in Pilar. We included Pilar standard libraries as well as GDPR, ISO/IEC 27002:2013 and ISO/IEC 29151:2017. We also specified the "target" phase to be achieved in one year. Naturally, the previous analysis within the threat modeling process was preparatory for this demonstration, as it offers a detailed and well-structured view of the elements to be included in the tool.

Each of the following sections is named as in the PILAR tool and according to the MAGERIT methodology.

7.4.1 Project (D)

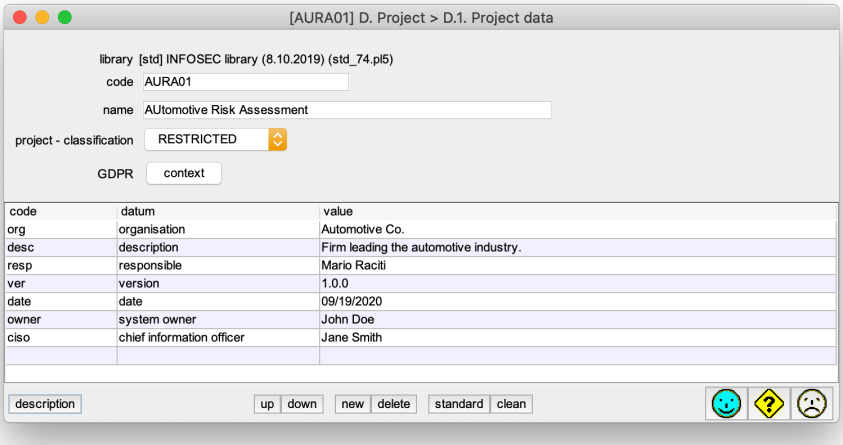


Figure 18: Project Data in Pilar

In this phase, we inserted the fictional values shown in Fig.18 in order to refer to our case study. We also added two security domains [MAGERIT - D.3] Car and Company to the Base domain — remember that we categorised assets in Car and Company domains except for Customer data (A0.1). Moreover, the remaining settings were left to their default values.

7.4.2 Risk Analysis (A)

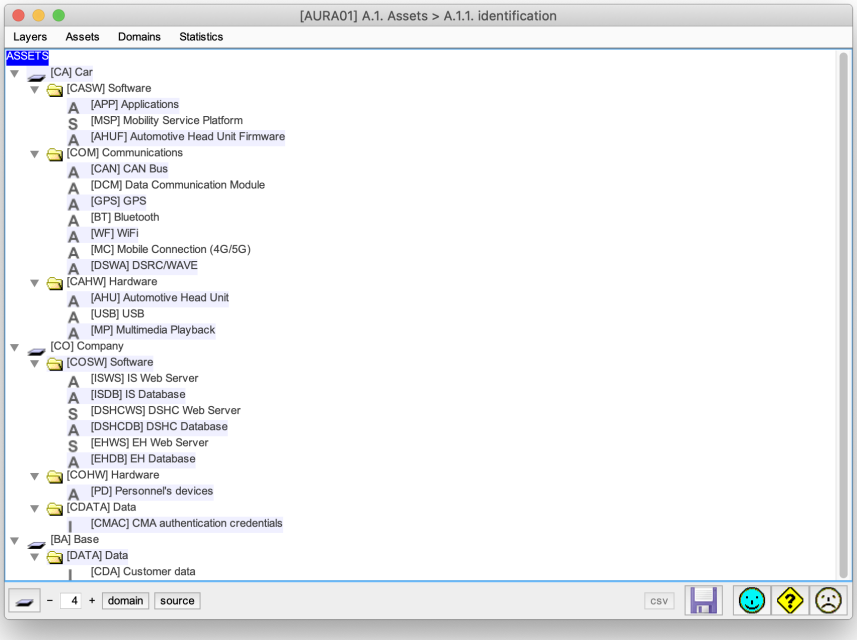


Figure 19: Assets Identification in Pilar

The process of Risk Analysis starts with assets identification. Since we had already performed such work employing the STRIDE threat model to our case study, we firstly proceeded to include the assets [MAGERIT - A.1.1] which have been identified in Tab.7 into Pilar, as Fig.19 depicts, according to the options that the tool itself offers.

The assets are grouped by two levels, which reflects the security domains themselves to simplify our work. It is important to highlight that we also marked as essential assets[24] the following ones: Mobility Service Platform (A2.3), Customer data (A0.1) , DSHC Web server (A1.3), EH Web server (A1.5), CMA authentication credentials (A1.7).

[24] In Sec.7.3.2 we gave a definition of essential assets according to Magerit.

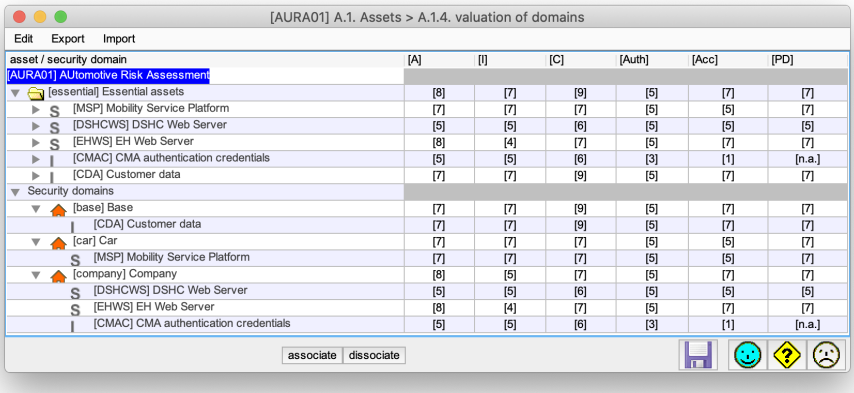


Figure 20: Valuation of Domains in Pilar

The next step [MAGERIT - A.1.4] involves the valuation of security domains as well as essential assets. In this process we had to value essential assets in the given dimensions[25]. Fortunately, Pilar helps us by providing several criteria, each of which is associated with a level between 0 and 10. In Fig.20 we can observe the values that we assigned to essential assets, including the relative accumulated values in the security domains.

As a sample, for the availability dimension of Mobility Service Platform (A2.3) we marked the "*[7] RTO < 4 hours*" as main criterion, since the MSP represents a core service for the entire automotive system. Moreover, for the confidentiality dimension of Customer data (A0.1) we assigned the "*[9] is likely to lead to an exceptionally serious breach of a legal or regulatory obligation*" as main parameter, because of the GDPR advices for personal data confidentiality. In general, each essential asset was marked according on the most suitable and reasonable options for it and its dimensions.

[25] Pilar offers Availability, Integrity, Confidentiality, Authenticity, Accountability, Value and Personal Data dimensions.

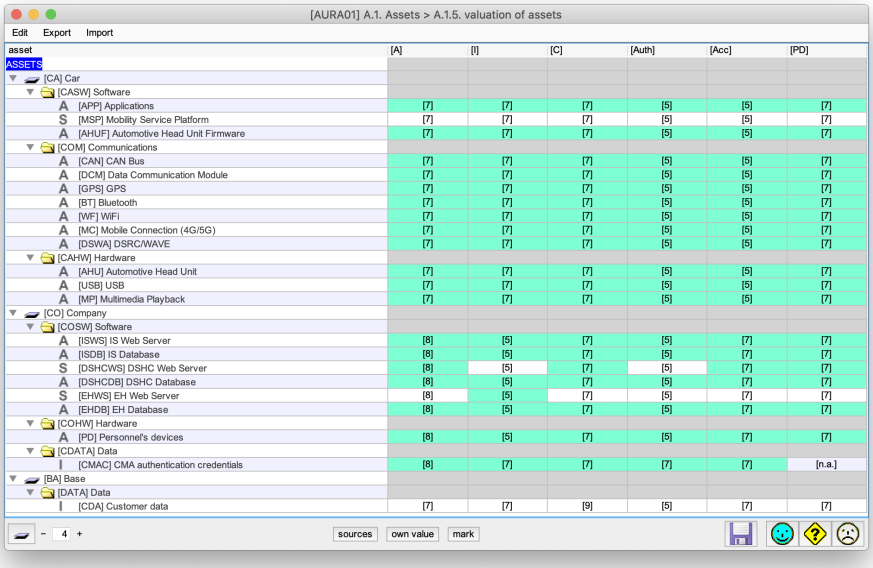


Figure 21: Valuation of Assets in Pilar

In general Pilar mainly offers two methods for assets valuation: *by domains* or *by assets*. In the latter case, you have to establish dependencies between assets which are used to propagate value (that is, security requirements) from valuable assets "above" onto equipment assets "below".

In our case study it was more convenient to use the first method[26], which propagates the values we have earlier set for essential assets to all the others, basing on the domain they belong to. Therefore, Fig.21 depicts as well as summarises the "assets valuation" step [MAGERIT - A.1.5], showing such accumulated value — that is what we also call propagation — in all of the three security domains for each dimension.

[26]It would be a stretch to try to bind many of the assets we have identified with dependencies.

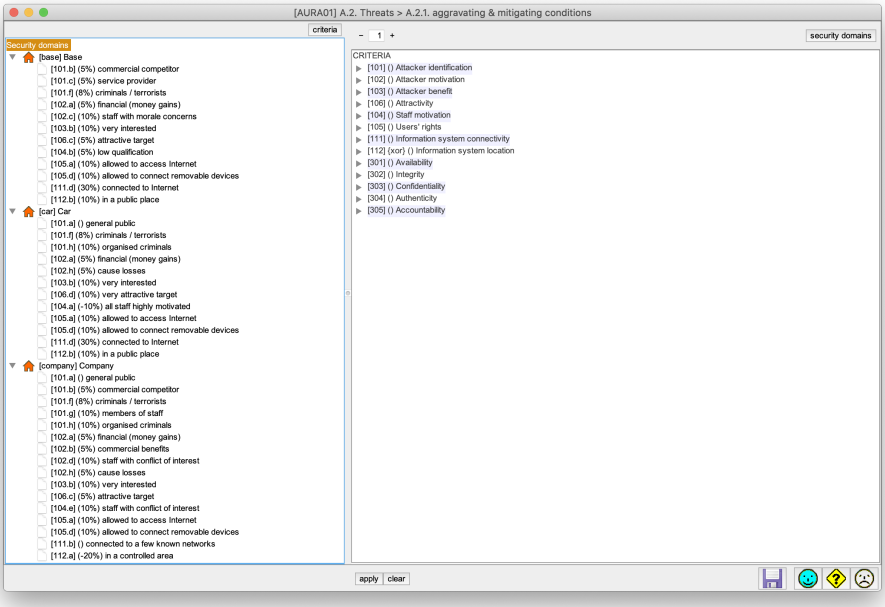


Figure 22: Aggravating and Mitigation Conditions in Pilar

Once we completed the foreseen phases, we proceeded to move on to threats [MAGERIT - A.2], making obvious reference to what threats were identified in the threat modeling work in Sec.7.3.4. Pilar automatically[27] associates threats to assets depending on the classes the latter belong to, choosing from five classes of threats: *[N] Natural, [I] Industrial, [E] Errors and unintentional failures, [A] Wilful attacks, [PR] Privacy risks*.

Before identifying threats, we firstly checked the values "aggravating and mitigating conditions" [MAGERIT - A.2.1] to be correctly assigned to each security domain. The tool initially proposed some default criteria, most of which were correctly associated to the three domains, reducing our work to just add or delete a couple of conditions — in Fig.22 a complete overview[28].

[27] It is important to note that, from this moment on, the tool automates many aspects.

[28] The threat agents we had prior identified are included as well.

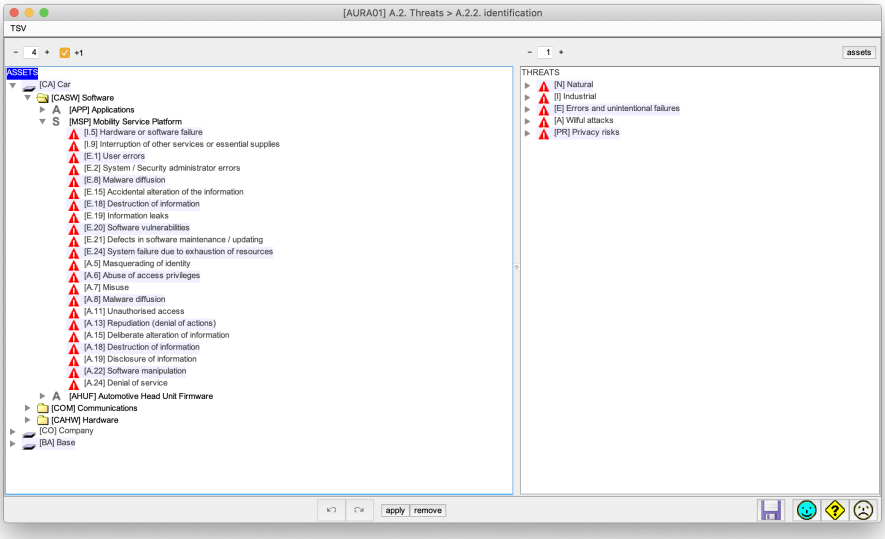


Figure 23: Threats Identification Sample in Pilar

Afterwards, in order to better identity the threats [MAGERIT - A.2.2], we performed a cross-analysis between the threats we had prior identified and those proposed automatically by Pilar. Fig.23 depicts a sample for the Mobility Service Platform (A2.3): as we can see all of the threats we had identified are covered. For instance, the threat regarding an unauthorised disclosure (T4.6) is embodied by both Information leaks [E.19] and Disclosure of information [A.19], the threat about a denial of service (T3.5) is represented by Denial of service [A.24], et cetera. Fortunately, as it is easy to understand, even in this case a few small changes to the list were enough.

After we completed the identification of threats we had to value them, similarly to the valuation process that we did for the assets, by assigning a likelihood value[29] and an effect (percentage) value for each dimension.

[29] Note that we set its representation by level: very low [VL], low [L], medium [M], high [H], very high [VH].

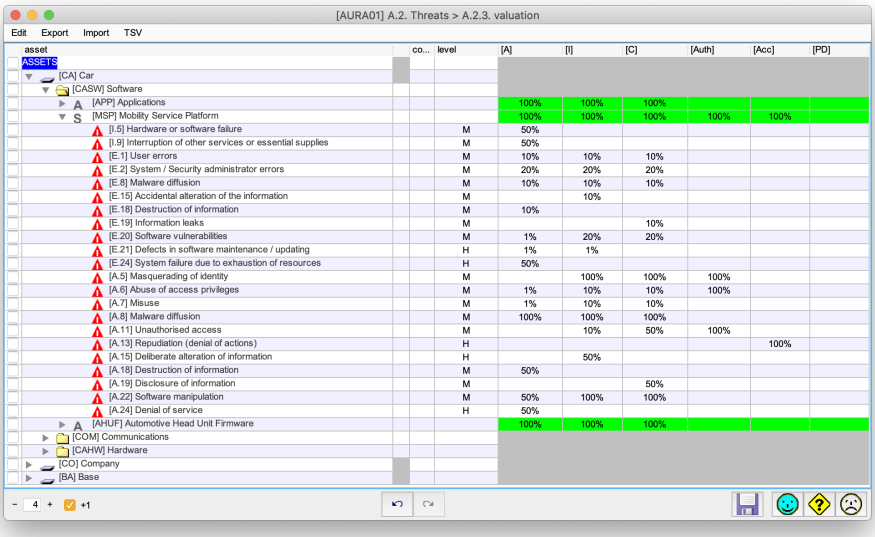


Figure 24: Valuation of Threats (Car domain) in Pilar

Regarding the valuation of the threats [MAGERIT - A.2.3], we started from the default values set by Pilar and we adapted these standard values to a likely scenario based on the likelihood and effect which most suited to the identified threats. Indeed, in this part of the analysis it is quite significant to consider a number of factors (e.g., threat agents, countermeasures[30], etc.) that influence likelihood and effect to avoid overdoing it resulting in a misjudgment. Similar to the example we reported earlier, Fig.24 shows a sample valuation of threats for the Mobility Service Platform (A2.3). As we can notice, for each row (identified threat) the likelihood values are included in the "level" column, whilst the effects are found in the columns relating to each dimension.

Since our study does not intend to focus on specific CVEs, we bypassed the insertion of these as well as "incidents"[31] [MAGERIT - A.2.4, A.2.5].

[30] Countermeasures will be treated in the next paragraph.

[31] In order not to burden our example we assumed that no incidents happened in the past.

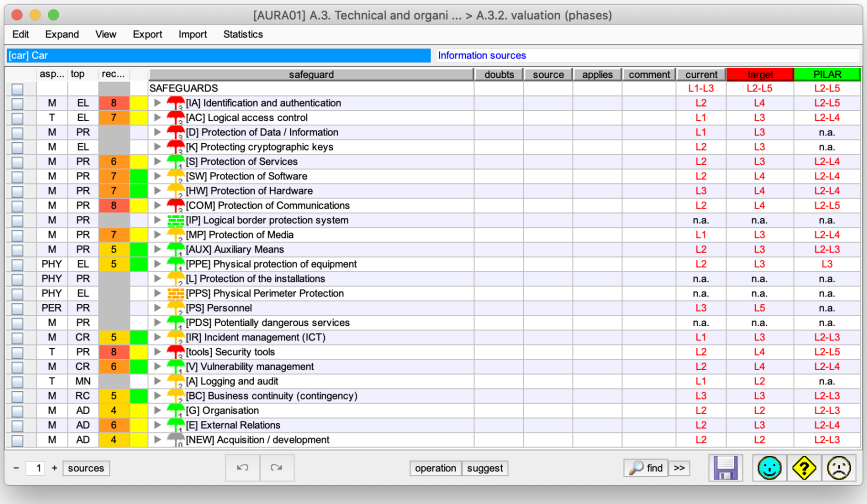


Figure 25: Valuation of Tech and organisational Measures Sample in Pilar

At this point of the risk analysis we have mostly considered negative factors that condition both the current impact value and, consequently, the current risk value — effectively making these values similar to potential[32] ones. Thus, we proceeded to the valuation of "Technical and organisational measures: Information security" [MAGERIT - A.3.2[33]]. This process consists of assigning a value of maturity — there are six choices: *n.a., L0: non-existent, L1: initial/ad hoc, L2: repeatable but intuitive, L3: defined process, L4: managed and measurable, L5: optimised* — to the safeguards for each project phase in all of the security domains.

In our case we hypothesised that the current phase started from quite elementary levels of maturity, with the aim of reaching the values suggested by Pilar. In Fig.25 we can observe the valuation for the Car domain.

[32]Remember that potential impact and potential risk are to be considered as the worst possible situations.

[33]Note that we proceeded by valuation by phases. It is also possible to do such work by domains [MAGERIT - A.3.3]

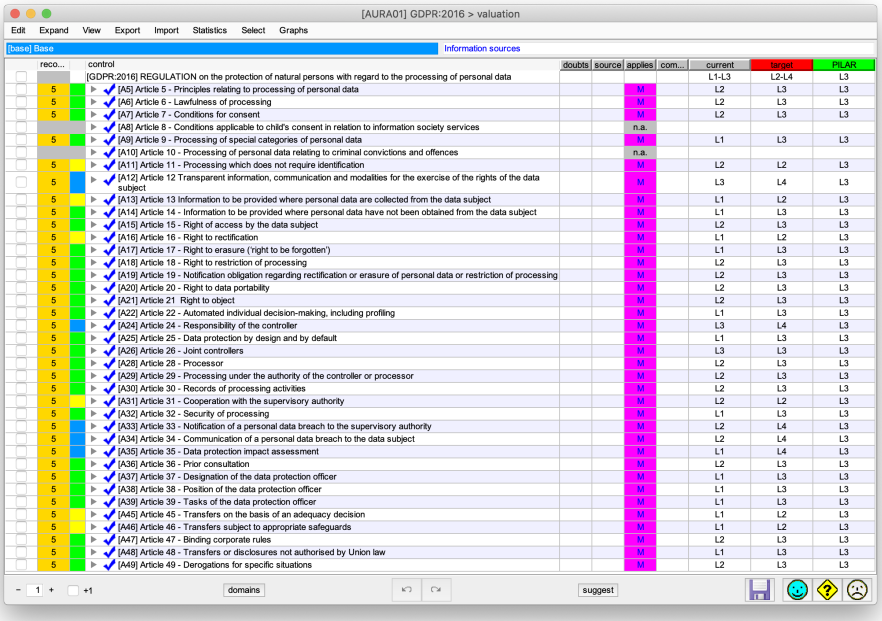


Figure 26: Valuation of GDPR (Base domain) in Pilar

In addiction to the technical and organisational measures, the tool also offers the possibility to perform a valuation of "Legal protection and compliance measures: Personal data" [MAGERIT - A.4]. Therefore, since we had included the GDPR and the ISO/IEC 29151:2017 libraries as security profiles, in this step we focused on the assessment of both the foreseen data protection regulation and *personal identifiable information (PII)* standard, along the lines of the previous step, by assigning the maturity level values for both the current and target phases, in the three security domains.

For instance, in Fig.26 a sample for the Base domain is shown. As can be noticed, we set a maturity level for each control[34] according to the most basic and reasonable maturity levels for the current phase, with the the aim of getting closer to the values proposed by Pilar.

[34]Remember that controls are main requirements from security profiles

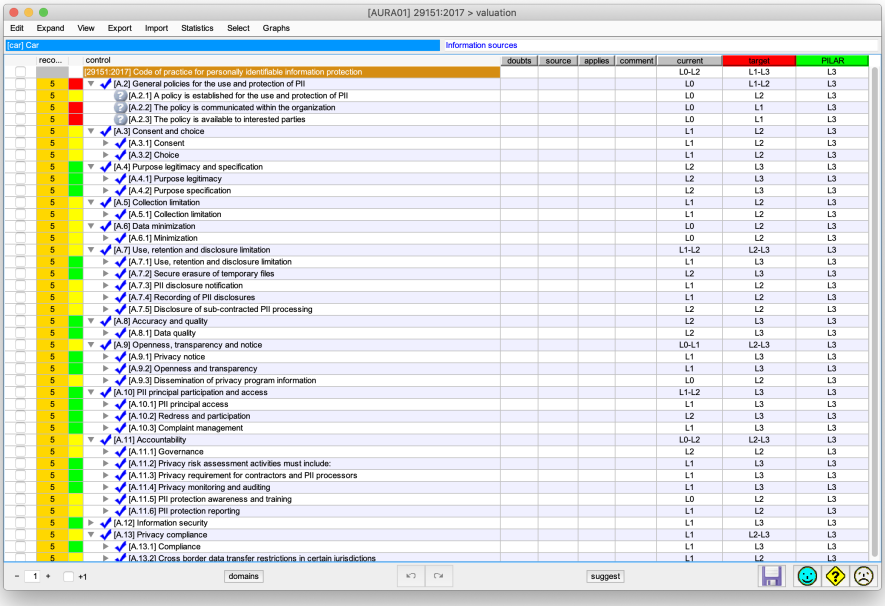


Figure 27: Valuation of ISO/IEC 29151:2017 (Car domain) in Pilar

Afterwards, we continued with the assignment of the maturity levels for the controls included in the ISO/IEC 29151:2017 in each of the three security domains. As a sample for such process, in Fig.27 the valuation for the Car domain is depicted

At this point, before proceeding to the "Impact & risk" [MAGERIT - A.6] step, in which the tool finally shows us the objective of the risk analysis — accumulated values and deflected values — it is important to remember that Pilar allows to perform the above assessments, for both the GDPR and the ISO/IEC 29151:2017 libraries, also in the Security profiles (E) phase. For this reason, the considerations regarding the compliance with these two security profiles are left to Sec.7.4.3, together with the compliance with the ISO/IEC 27002:2013 library, which assessment is instead presented below as the maturity values of its controls influence the results of our analysis.

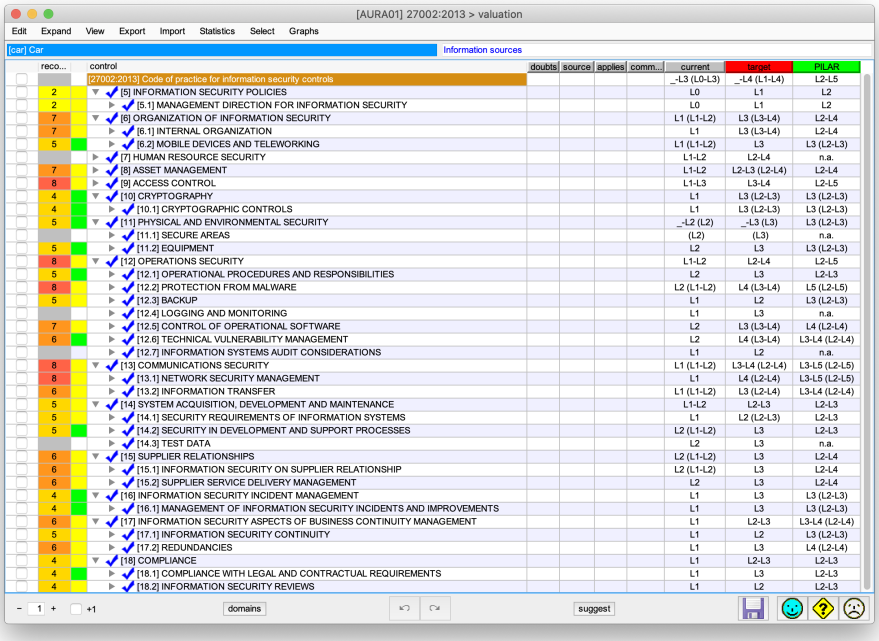


Figure 28: Valuation of ISO/IEC 27002:2013 (Car domain) in Pilar

We indeed completed the assessment of both positive and negative measures within the valuation of the "Code of practice for information security controls" [ISO/IEC 27002:2013], again by assigning the maturity levels for all three domains. In Fig.28 a sample for the Car domain is illustrated.

This last assessment process concludes what we can define as the "data entry" phase, as we are eventually ready to analyse the results which Pilar calculated basing on the data we had inserted in the previous phases. Therefore, now that we have considered all the factors that influence impacts and risks, both for essential and inferior assets, we can finally compare the accumulated values and deflected values among in the four phases: potential, current, target and PILAR.

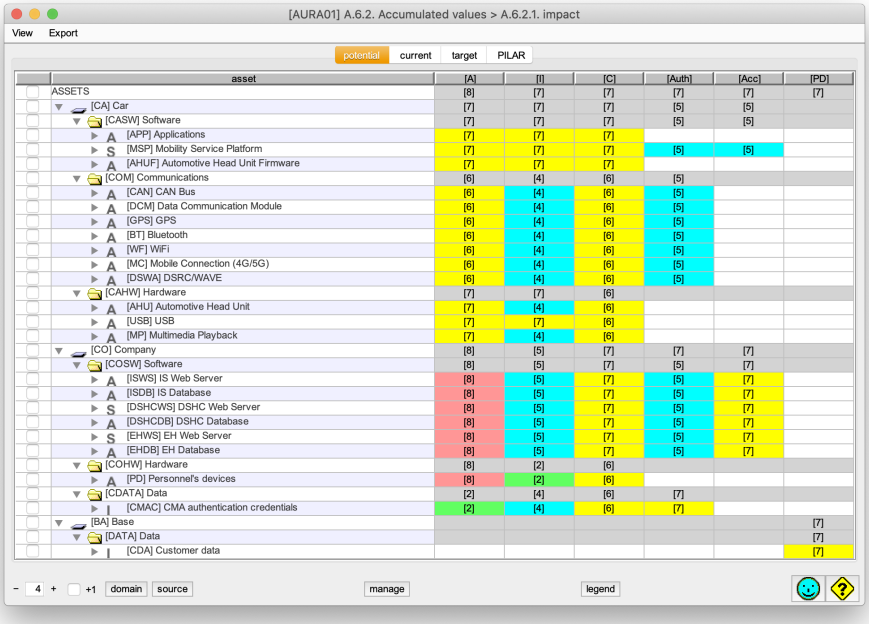


Figure 29: Potential Accumulated Impact in Pilar

Caveat: accumulated impact is calculated for an asset taking into account its accumulated value (its own plus the accumulated value of the assets that depend on it) and the threats which it is exposed to.

Since we proceed according to the steps provided by Magerit, firstly we discuss accumulated values. In particular, we present the accumulated impact [MAGERIT - A.6.2.1] in the potential phase in Fig.29, emphasising the severity in the worst possible case without considering measures and protections. As we can observe, the highest values of potential accumulated impact are present in the availability dimension — especially in the Company domain with a value of 8 —, followed by respectively the confidentiality and personal data dimensions.

Although, the accumulated impact significantly reduces in the current phase, as it is depicted in Fig.30, because of the considered measures and protec-

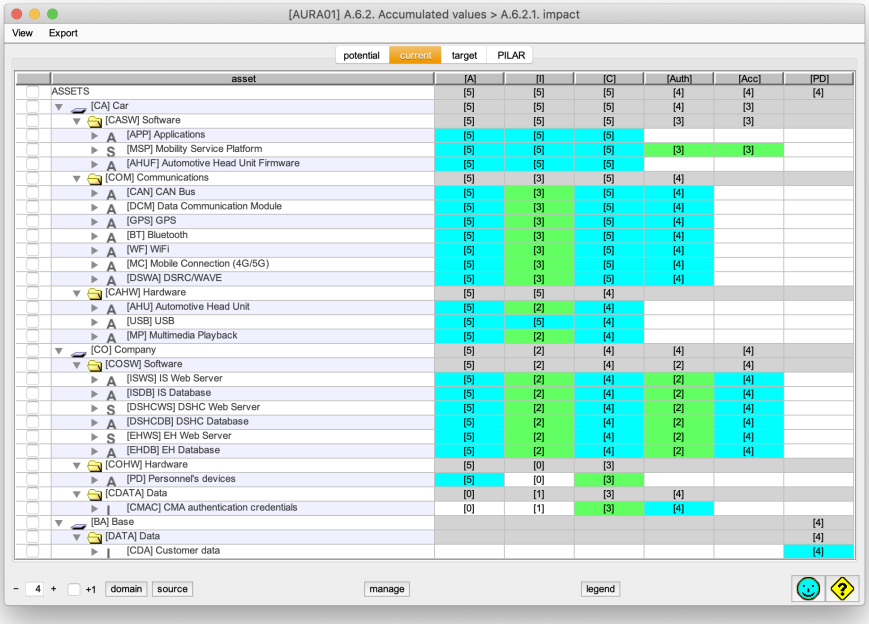


Figure 30: Current Accumulated Impact in Pilar

tions. This fact results in a flattening of the prior differences between the Car and Company domains. It is obvious that these values are further reduced in the target phase, as we can see in Fig.31, where the values are between 2 and 3. This means that the accumulated impact values are between low and medium on the scale[35].

At this point we can conclude the analysis of the results for the accumulated impact by observing that the values in the target phase are almost equivalent to those recommended by the tool — shown in Fig32 —, id est in the PILAR phase. It is important to clarify that this is mainly due to the assumptions and assignments that we made in the previous assessment steps, by partially following Pilar suggestions.

[35]Remember that this scale ranges between 0 and 10.

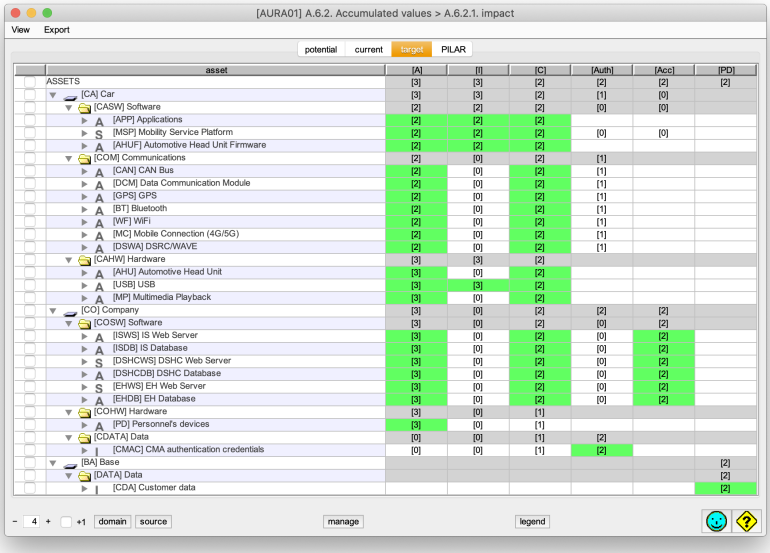


Figure 31: Target Accumulated Impact in Pilar

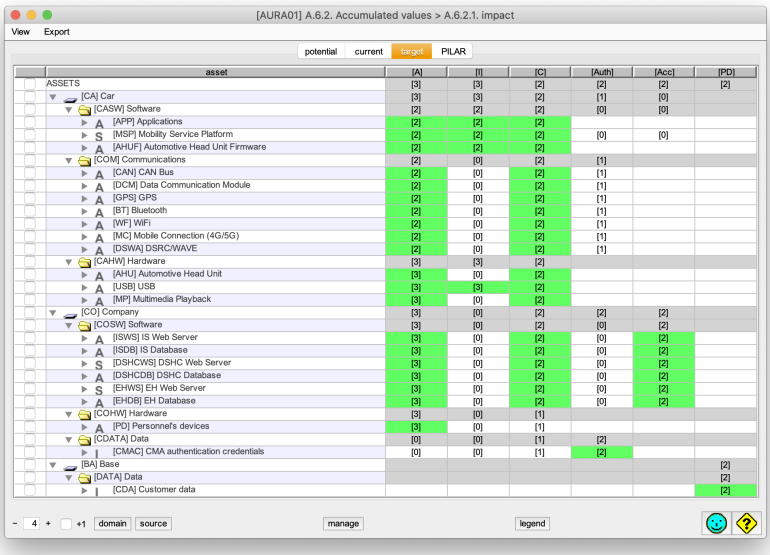


Figure 32: PILAR Accumulated Impact in Pilar

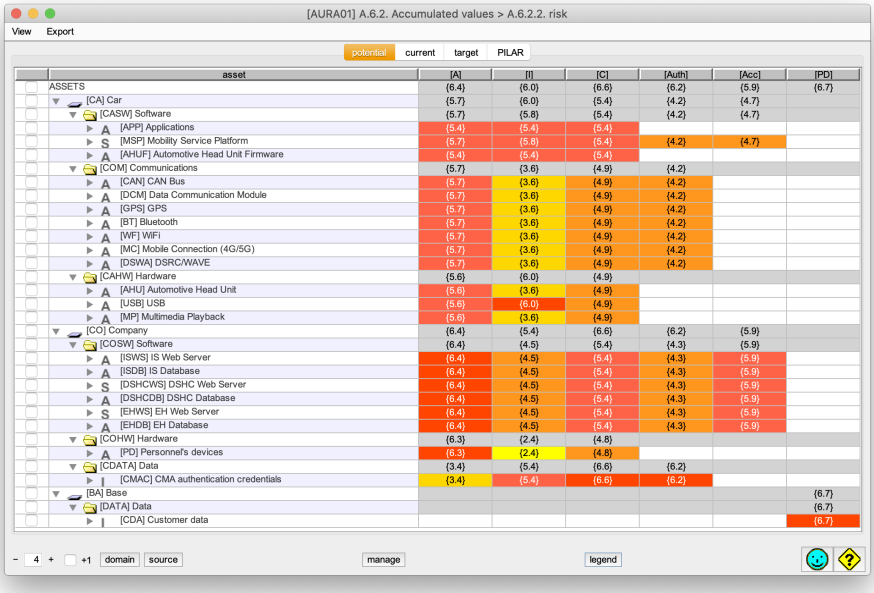


Figure 33: Potential Accumulated Risk in Pilar

Caveat: accumulated risk is calculated for an asset taking into account the accumulated impact on an asset arising from a threat and the likelihood of threats.

Similarly to the previous comparisons, we can proceed to the analysis of the accumulated risk [MAGERIT - A.6.2.2] by proposing these values[36] in the potential phase in Fig.33. Seeing as we are flooded with a mostly red overview, it can be deduced that the accumulated risk values are quite high. As a matter of fact they are — the values are mostly classified as critical and very critical. Nevertheless it is a situation, as we recall, which the measures as well as protections are not contemplated in.

The actual situation, represented by the current phase and depicted in Fig.34, appears less dramatic.

[36]Note that the scale here is between 0 and 9, unlike the prior case.

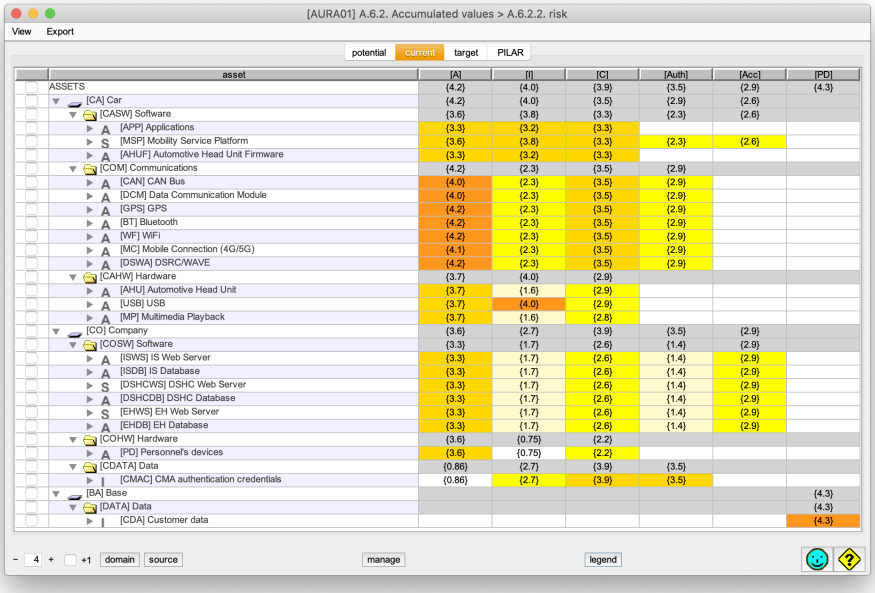


Figure 34: Current Accumulated Risk in Pilar

However it should not be underestimated given that several values are classified as "{4} - very high", especially for the Communications [COM] assets in the Car domain and the Customer data (A0.1), as we expected from the initial phases of the risk analysis.

Also in this case, the accumulated risk values in the target and PILAR phases are strictly close. Furthermore, accumulated risk results, in an ambitious manner, significantly reduced — as Fig.35 illustrates — compared to its values in the current phase. Eventually, speaking of the target phase, it is important to explain that the accumulated risk values of the assets in the Company domain result a bit lower than their counterparts in the PILAR phase, depicted by Fig.36, because of our assumption that the Company domain was intended to be more secure than the Car one as the current phase in Fig.34 shows, too.

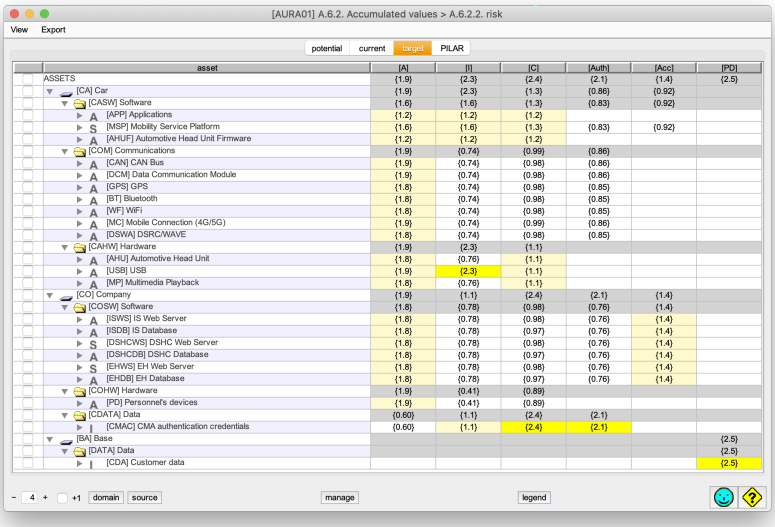


Figure 35: Target Accumulated Risk in Pilar

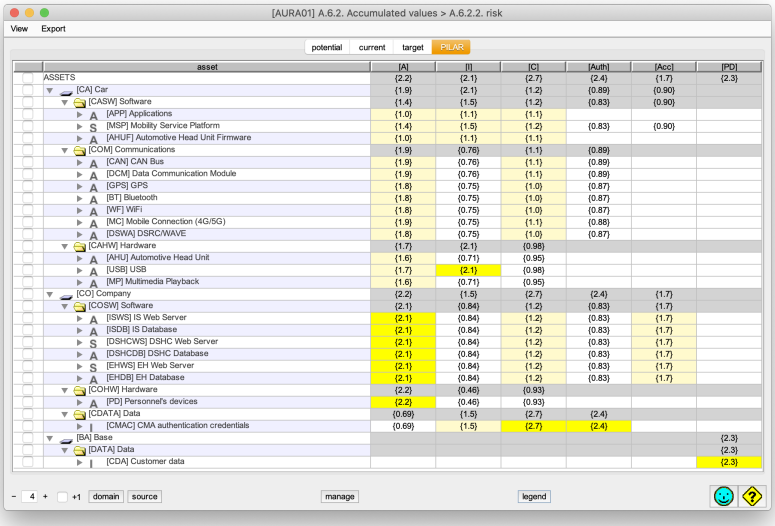
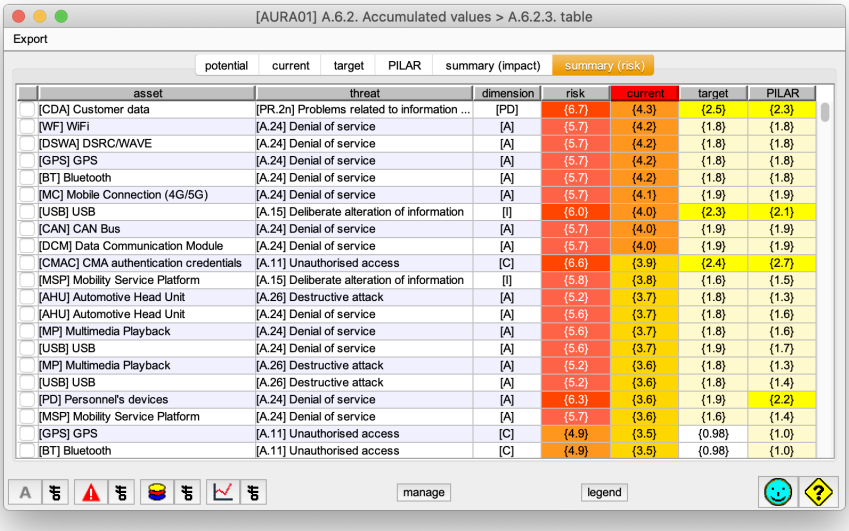


Figure 36: PILAR Accumulated Risk in Pilar



asset	threat	dimension	risk	current	target	PILAR
[CDA] Customer data	[PR.2n] Problems related to information ...	[PD]	{6.7}	{4.3}	{2.5}	{2.3}
[WF] WiFi	[A.24] Denial of service	[A]	{5.7}	{4.2}	{1.8}	{1.8}
[DSWA] DSRC/WAVE	[A.24] Denial of service	[A]	{5.7}	{4.2}	{1.8}	{1.8}
[GPS] GPS	[A.24] Denial of service	[A]	{5.7}	{4.2}	{1.8}	{1.8}
[BT] Bluetooth	[A.24] Denial of service	[A]	{5.7}	{4.2}	{1.8}	{1.8}
[MC] Mobile Connection (4G/5G)	[A.24] Denial of service	[A]	{5.7}	{4.1}	{1.9}	{1.9}
[USB] USB	[A.15] Deliberate alteration of information	[I]	{6.0}	{4.0}	{2.3}	{2.1}
[CAN] CAN Bus	[A.24] Denial of service	[A]	{5.7}	{4.0}	{1.9}	{1.9}
[DCM] Data Communication Module	[A.24] Denial of service	[A]	{5.7}	{4.0}	{1.9}	{1.9}
[CMAC] CMA authentication credentials	[A.11] Unauthorised access	[C]	{6.6}	{3.9}	{2.4}	{2.7}
[MSP] Mobility Service Platform	[A.15] Deliberate alteration of information	[I]	{5.8}	{3.8}	{1.6}	{1.5}
[AHU] Automotive Head Unit	[A.26] Destructive attack	[A]	{5.2}	{3.7}	{1.8}	{1.3}
[AHU] Automotive Head Unit	[A.24] Denial of service	[A]	{5.6}	{3.7}	{1.8}	{1.6}
[MP] Multimedia Playback	[A.24] Denial of service	[A]	{5.6}	{3.7}	{1.8}	{1.6}
[USB] USB	[A.24] Denial of service	[A]	{5.6}	{3.7}	{1.9}	{1.7}
[MP] Multimedia Playback	[A.26] Destructive attack	[A]	{5.2}	{3.6}	{1.8}	{1.3}
[USB] USB	[A.26] Destructive attack	[A]	{5.2}	{3.6}	{1.8}	{1.4}
[PD] Personnel's devices	[A.24] Denial of service	[A]	{6.3}	{3.6}	{1.9}	{2.2}
[MSP] Mobility Service Platform	[A.24] Denial of service	[A]	{5.7}	{3.6}	{1.6}	{1.4}
[GPS] GPS	[A.11] Unauthorised access	[C]	{4.9}	{3.5}	{0.98}	{1.0}
[BT] Bluetooth	[A.11] Unauthorised access	[C]	{4.9}	{3.5}	{0.98}	{1.0}

Figure 37: Accumulated Risk Summary in Pilar

Definitely, we can observe a summary for accumulated risk in Fig.37 which helps to realise that the major threats for our case study are represented by denial of service, unauthorised access and issues involving information.

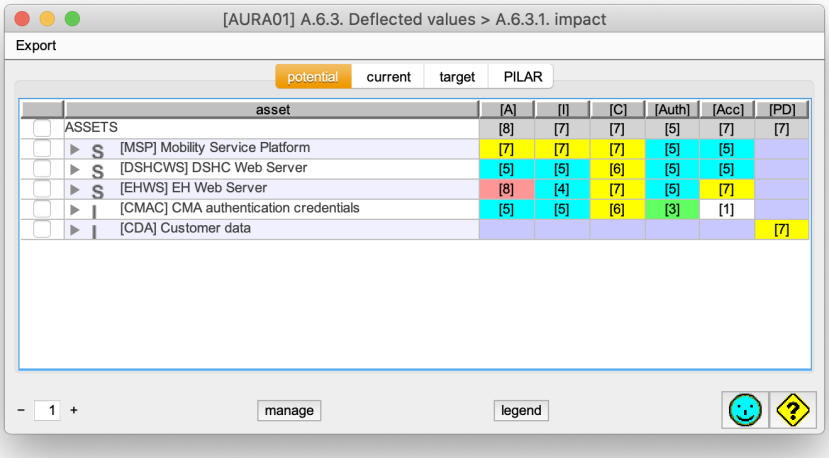


Figure 38: Potential Deflected Impact in Pilar

Caveat: deflected impact is calculated for an asset taking into account its intrinsic value and the threats which the assets on which it depends are exposed to.

We reach the end of the Risk Analysis [MAGERIT - A] phase by proceeding with an analogous modus operandi for the deflected values. Particularly, deflected impact values [MAGERIT - A.6.3.1] shown in Fig.38 highlight the Mobility Service Platform (A2.3), the Emergency Helpnet Web Server (A1.5) and the Customer data (A0.1) as the most critical values of deflected impact amongst essential assets.

Current deflected impact confirms the foreseen considerations made regarding the potential case, with a reduction of the values as well as expected. In order to compare some of the most important results by observing what is depicted in Fig.39, we can note that the CMA authentication credentials (A1.7) asset actually has a lower value of deflected impact compared to the Mobility Service Platform (A2.3).

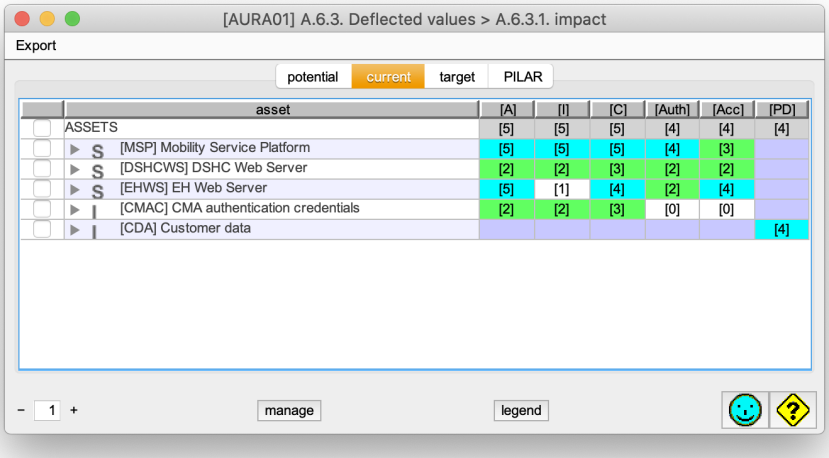


Figure 39: Current Deflected Impact in Pilar

The reason of the above distinction lies — as we already mentioned it in Sec.7.3.4 — in the importance of the impact: the former asset may involve a single user, whilst the latter might possibly affects all the customers connected to its network.

Target and PILAR deflected impact values, similarly to what happened for accumulated impact, are strictly close each other. We can observe these values, respectively, in Fig.40 and Fig.41. Although, a clarification has to be presented: the deflected impact value for the EH Web Server (A1.5) asset results higher in the suggested phase compared to the target phase. Intuitively, this fact is especially influenced by the robust measures and protections assumed to a critical asset as the EH Web Server — remember that it might affect customers' safety.

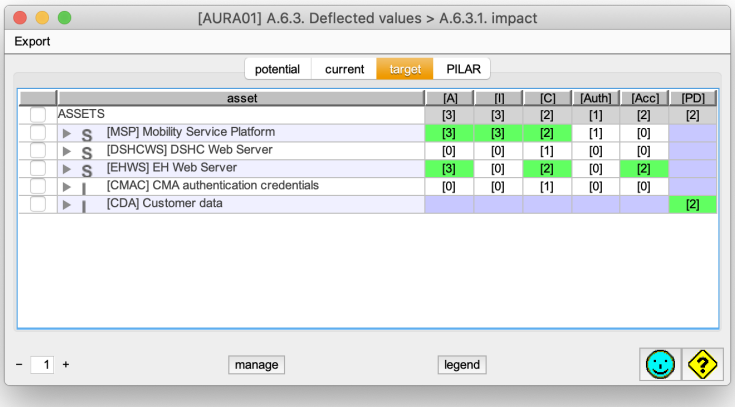


Figure 40: Target Deflected Impact in Pilar

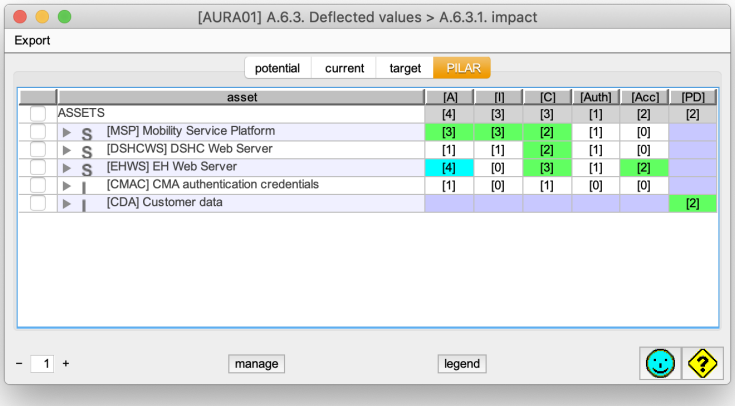


Figure 41: PILAR Deflected Impact in Pilar

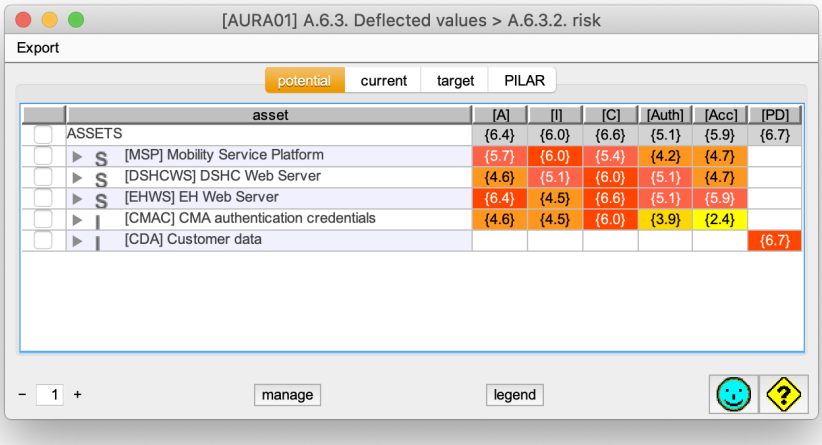


Figure 42: Potential Deflected Risk in Pilar

Caveat: deflected risk is calculated for an asset taking into account the deflected impact on an asset due to a threat and the likelihood of the threat.

The other side of the coin, deflected risk [MAGERIT - A.6.3.2] depicted in Fig.42, introduces the risks in essential assets in the potential phase — here the scene is once again stained with red. As we can note, the confidentiality and personal data dimensions appear to be the most critical ones in each of the five[37] essential assets.

The situation appears to be decreased by a couple of points in current deflected risk, where Fig.43 illustrates that the most critical values regard the availability ("{4.2} - very high") and integrity ("{4.3} - very high") dimensions for the Mobility Service Platform (A2.) asset, as well as the confidentiality dimension in every asset. Moreover, the personal data dimension for the Customer data (A0.1) asset still remains the top-ranked with a deflected

[37] To be more exact, confidentiality for the first four assets, whilst personal data for the Customer data (A0.1) asset.

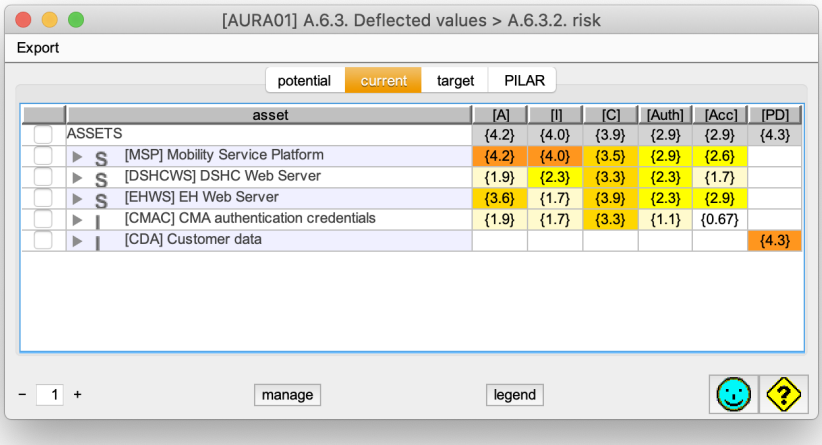


Figure 43: Current Deflected Risk in Pilar

risk value of "{4.3} - very high".

We can eventually compare the target and PILAR deflected risk values. These are depicted, respectively, in Fig.44 and Fig.45. Once again, the results in both phases are quite close since our aim is to minimise the risks, also by following the suggestions of the tool. Furthermore, it is obvious that in the Risk Management phase we should prioritise the most critical dimensions, such as availability, confidentiality and personal data, emerged by these analyses.

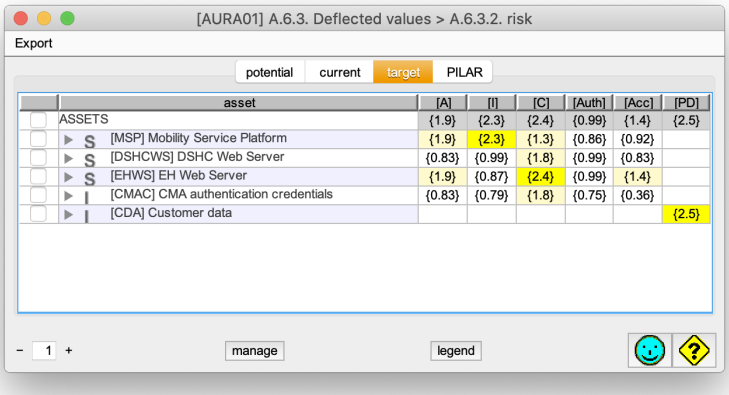


Figure 44: Target Deflected Risk in Pilar

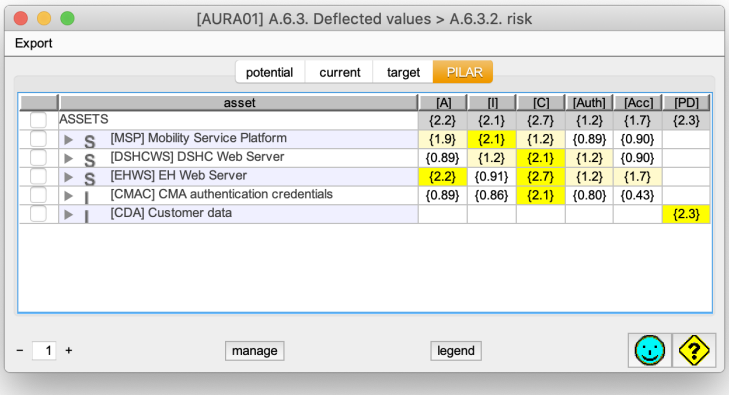
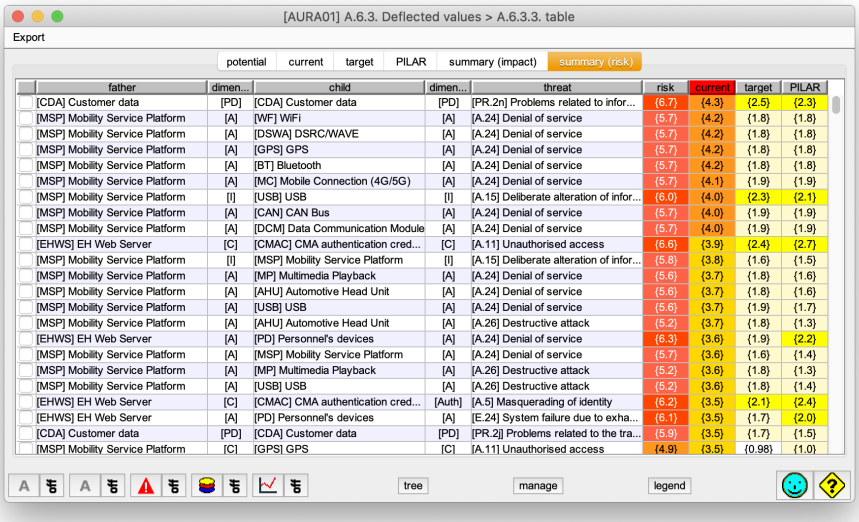


Figure 45: PILAR Deflected Risk in Pilar



father	dimen...	child	dimen...	threat	risk	current	target	PILAR
[CDA] Customer data	[PD]	[CDA] Customer data	[PD]	[PR.2n] Problems related to infor...	{6.7}	{4.3}	{2.5}	{2.3}
[MSP] Mobility Service Platform	[A]	[WF] WiFi	[A]	[A.24] Denial of service	{5.7}	{4.2}	{1.8}	{1.8}
[MSP] Mobility Service Platform	[A]	[DSWA] DSRC/WAVE	[A]	[A.24] Denial of service	{5.7}	{4.2}	{1.8}	{1.8}
[MSP] Mobility Service Platform	[A]	[GPS] GPS	[A]	[A.24] Denial of service	{5.7}	{4.2}	{1.8}	{1.8}
[MSP] Mobility Service Platform	[A]	[BT] Bluetooth	[A]	[A.24] Denial of service	{5.7}	{4.2}	{1.8}	{1.8}
[MSP] Mobility Service Platform	[A]	[MC] Mobile Connection (4G/5G)	[A]	[A.24] Denial of service	{5.7}	{4.1}	{1.9}	{1.9}
[MSP] Mobility Service Platform	[I]	[USB] USB	[I]	[A.15] Deliberate alteration of infor...	{6.0}	{4.0}	{2.3}	{2.1}
[MSP] Mobility Service Platform	[A]	[CAN] CAN Bus	[A]	[A.24] Denial of service	{5.7}	{4.0}	{1.9}	{1.9}
[MSP] Mobility Service Platform	[A]	[DCM] Data Communication Module	[A]	[A.24] Denial of service	{5.7}	{4.0}	{1.9}	{1.9}
[EHWS] EH Web Server	[C]	[CMAC] CMA authentication cred...	[C]	[A.11] Unauthorised access	{6.6}	{3.9}	{2.4}	{2.7}
[MSP] Mobility Service Platform	[I]	[MSP] Mobility Service Platform	[I]	[A.15] Deliberate alteration of infor...	{5.8}	{3.8}	{1.6}	{1.5}
[MSP] Mobility Service Platform	[A]	[MP] Multimedia Playback	[A]	[A.24] Denial of service	{5.6}	{3.7}	{1.8}	{1.6}
[MSP] Mobility Service Platform	[A]	[AHU] Automotive Head Unit	[A]	[A.24] Denial of service	{5.6}	{3.7}	{1.8}	{1.6}
[MSP] Mobility Service Platform	[A]	[USB] USB	[A]	[A.24] Denial of service	{5.6}	{3.7}	{1.9}	{1.7}
[MSP] Mobility Service Platform	[A]	[AHU] Automotive Head Unit	[A]	[A.26] Destructive attack	{5.2}	{3.7}	{1.8}	{1.3}
[EHWS] EH Web Server	[A]	[PD] Personnel's devices	[A]	[A.24] Denial of service	{6.3}	{3.6}	{1.9}	{2.2}
[MSP] Mobility Service Platform	[A]	[MSP] Mobility Service Platform	[A]	[A.24] Denial of service	{5.7}	{3.6}	{1.6}	{1.4}
[MSP] Mobility Service Platform	[A]	[MP] Multimedia Playback	[A]	[A.26] Destructive attack	{5.2}	{3.6}	{1.8}	{1.3}
[MSP] Mobility Service Platform	[A]	[USB] USB	[A]	[A.26] Destructive attack	{5.2}	{3.6}	{1.8}	{1.4}
[EHWS] EH Web Server	[C]	[CMAC] CMA authentication cred...	[Auth]	[A.5] Masquerading of identity	{6.2}	{3.5}	{2.1}	{2.4}
[EHWS] EH Web Server	[A]	[PD] Personnel's devices	[A]	[E.24] System failure due to exha...	{6.1}	{3.5}	{1.7}	{2.0}
[CDA] Customer data	[PD]	[CDA] Customer data	[PD]	[PR.2j] Problems related to the tra...	{5.9}	{3.5}	{1.7}	{1.5}
[MSP] Mobility Service Platform	[C]	[GPS] GPS	[C]	[A.11] Unauthorised access	{4.9}	{3.5}	{0.98}	{1.0}

Figure 46: Deflected Risk Summary in Pilar

Definitely, we can observe a summary for deflected risk in Fig.46 which helps to realise how that the major threats of inferior assets (i.e., denial of service, unauthorised access and issues involving information) are propagated up to their parents, distinguishing their high values of risk. Ultimately, it should be emphasised that, even in this case, we have yet another proof that the assets belonging to the Car domain are the most critical.

7.4.3 Reports (R)

The previous section produced several results which have been analysed singularly. Now we can review the obtained data as well as compare the different phases — potential, current, target and PILAR — of our case study according to multiple factors.

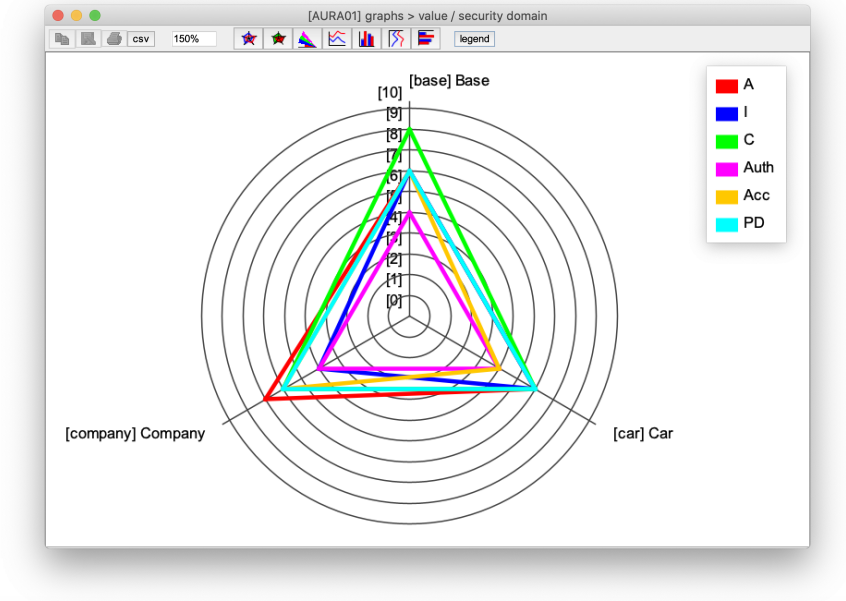


Figure 47: Value of Assets per Domain in Pilar

Thus, accordingly to the steps provided by Magerit, we can start to analyse the graph illustrating the values of each asset. Thus, in Fig.47 we can observe that the availability dimension is highly valued in both the Company and the Car domain, whilst the confidentiality dimension stands out in the Base domain, especially. It follows the personal data dimension.

Safeguards are the next data to glance at in our report. These values are depicted in Fig.48 concerning aspects and in Fig.49 regarding strategies. In particular, "technical safeguards [T]" represents a factor to keep an eye on, as well as the "reduce impact [RI]" and "recover [R]" strategies.

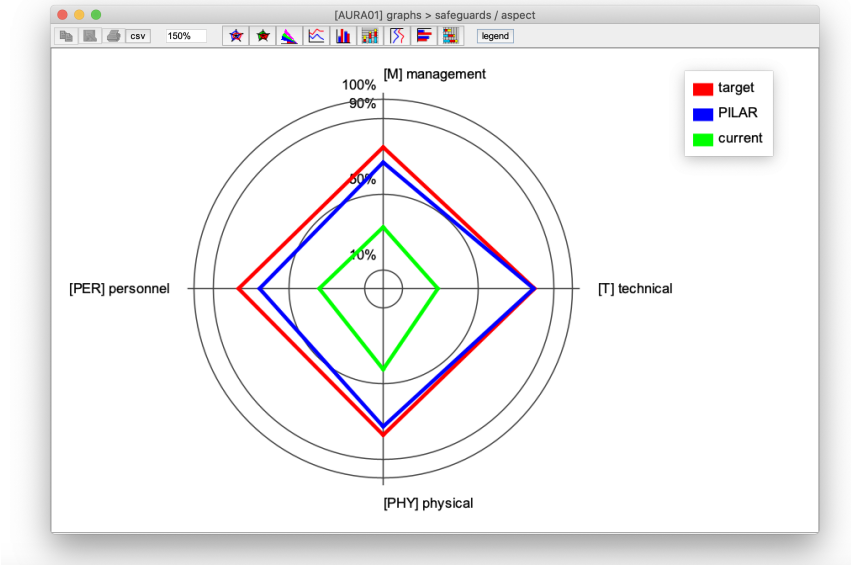


Figure 48: Safeguards per Aspect in Pilar

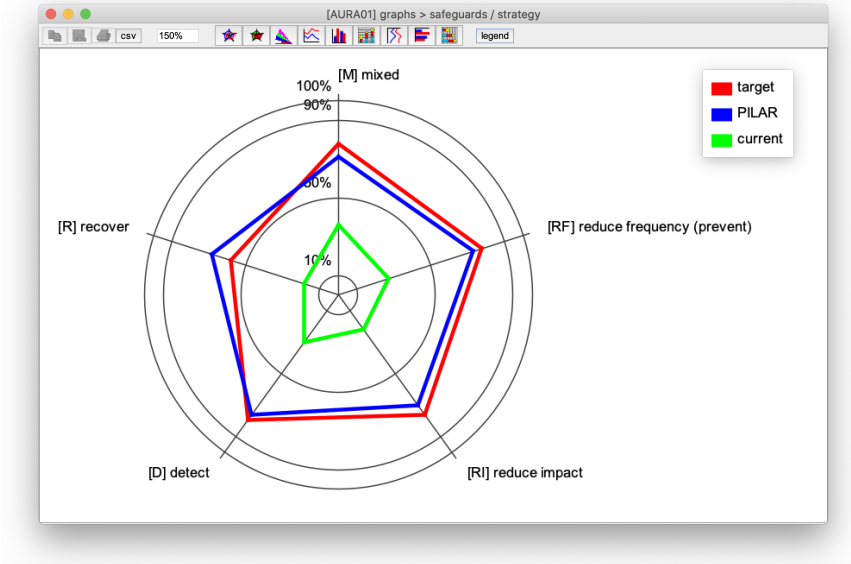


Figure 49: Safeguards per Strategy in Pilar

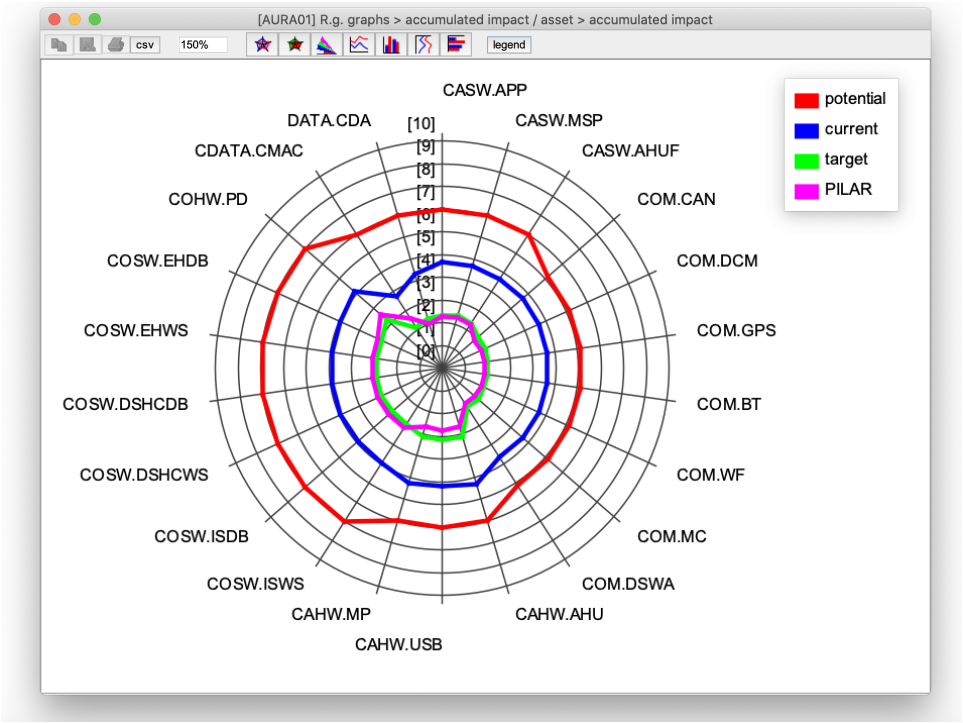


Figure 50: Accumulated Impact Comparison in Pilar

Successively we can analyse the values of accumulated impact in the four phases. As Fig.50 shows, it results now more clear how the initial predominance of accumulated impact values, in the potential phase for the assets in the Company domain, shifts in the current phase for the assets in the Car domain. In other words, from a potential prevalence of values in the left side of the graph, the situation overturns into the current phase, where the blue line is mostly inclined to the right side.

As a result, the target accumulated impact values appear to be especially reduced in the Car domain, compared to the current phase and, as we prior disclosed, they are strictly close to those in the PILAR phase. We can also glance at accumulated impact by dimensions referring to Fig.52, where the CIA triad dimensions present the highest values in the current phase.

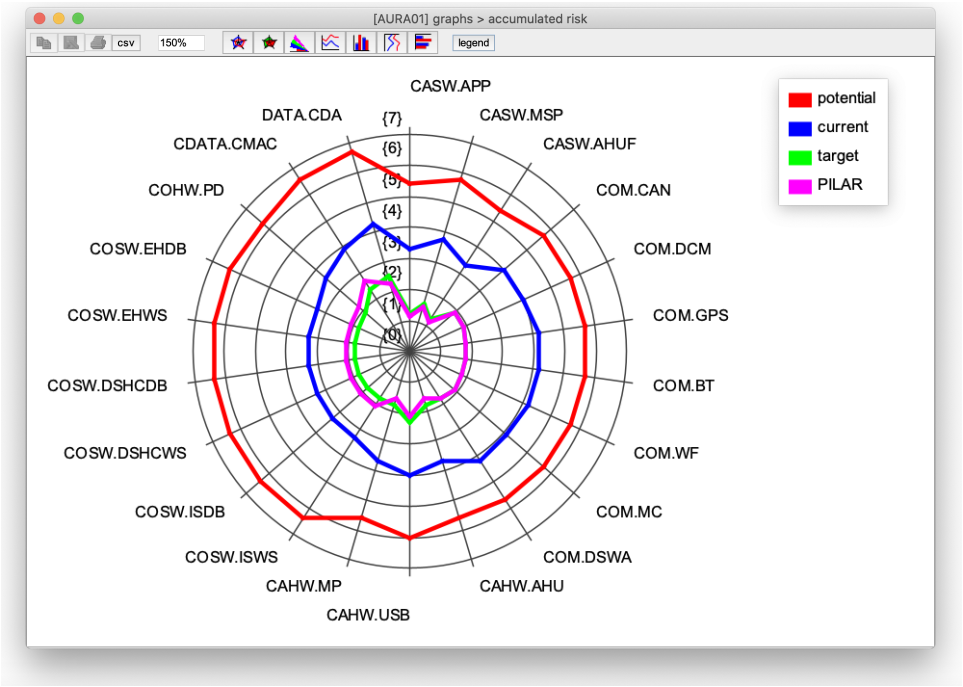


Figure 51: Accumulated Risk Comparison in Pilar

Accumulated risk in the four phases can be observed in Fig.51. From the difference between the shape of the red line and the shape of the blue one, similarly to the case of accumulated impact, it results emphasised that accumulated risk values for the assets in the Car domain are rather close to the corresponding potential values. In addiction, by noticing from the green line, the maturity level values for safeguards and protections, which we set for the target phase, contribute to decrease accumulated risk values that become almost purely close to those suggested by Pilar.

As a result, the graph suggests that a primary effort for a reduction of accumulated risk should be performed in the Car domain. Eventually, we can also glance at accumulated risk by dimensions referring to Fig.53, in which the personal data and CIA triad dimensions come with the highest values in the current phase.

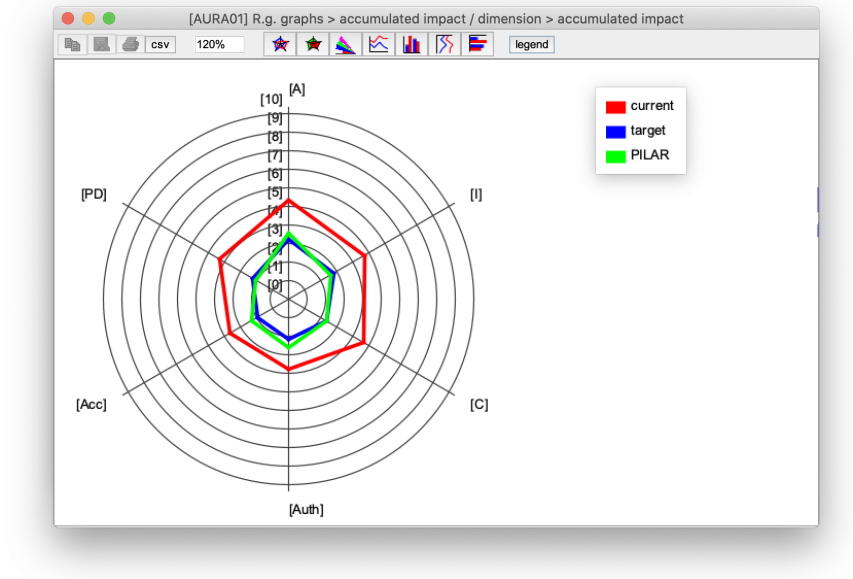


Figure 52: Accumulated Impact per Dimension in Pilar

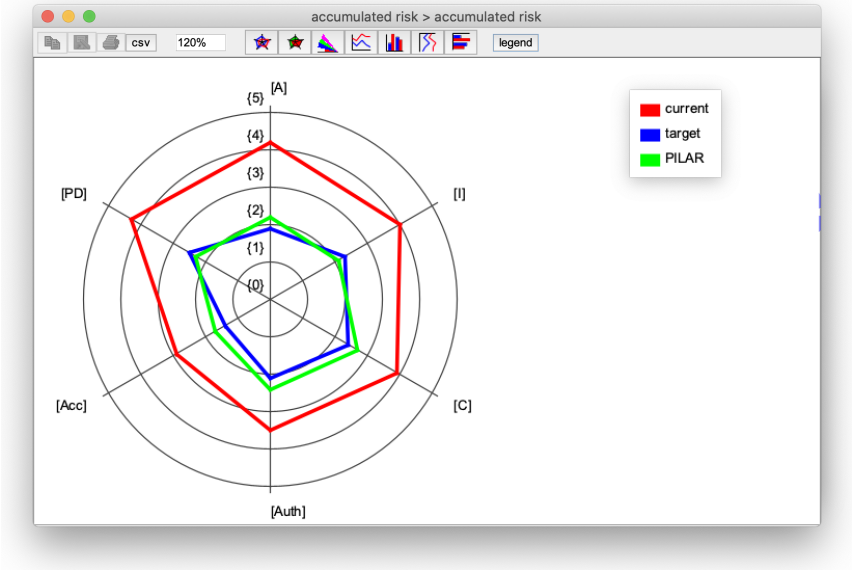


Figure 53: Accumulated Risk per Dimension in Pilar

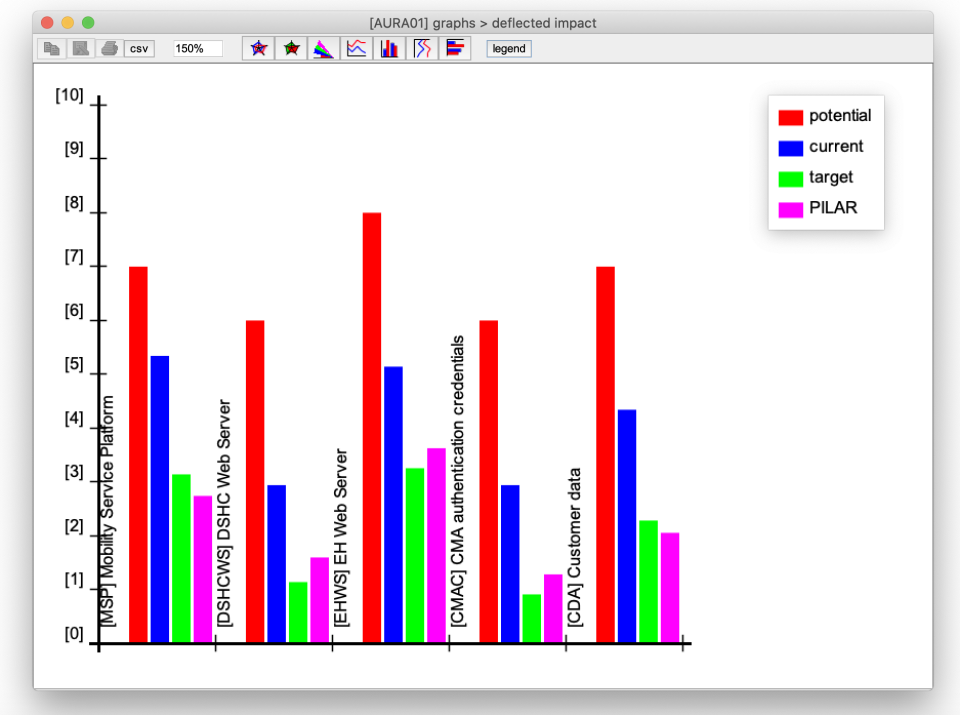


Figure 54: Deflected Impact Comparison A in Pilar

Now we can proceed to observe deflected impact values, depicted in Fig.54, to analyse the relevance of essential assets in the four phases. From a first overview we can deduce that the DSHC Web server (A1.3) and CMA authentication credentials (A1.7) assets can be moved to the background, compared with the remaining ones. Indeed, the potential phase for this two essential assets is sufficiently distant from the current phase.

As a last note about deflected impact, Fig.56 better illustrates how from a "quasi-regular pentagonal" situation, in potential and current phases, accumulated impact values take the shape of a triangle in target and PILAR phases. Thereby three essential assets are particularly highlighted as the most relevant and potentially critical: Mobility Service Platform (A2.3), EH Web server (A1.5) and Customer data (A0.1).

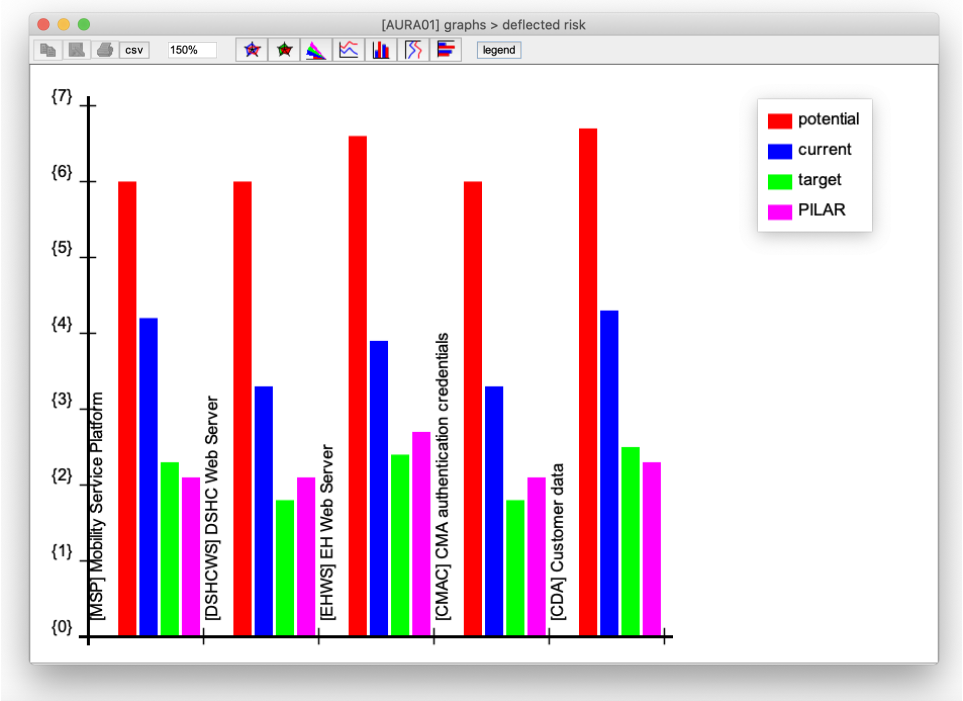


Figure 55: Deflected Risk Comparison A in Pilar

In conclusion, we can analyse deflected risk values shown in Fig.55. If the case of deflected impact appears to be divided into two parts (i.e., three essential assets with highest impact than the remaining), here the situation looks more homogeneous in all of the four phases. Despite the major deflected risk values result — as we expected from the previous analyses — in proximity of the three essential assets mentioned in the last paragraph[38], the difference of current deflected risk values between essential assets is quite minimal — it ranges in the interval [3, 4.5]. Even in this case, note that the target and PILAR phases are almost overlapping.

Eventually, a generic view of the four phases is illustrated in Fig.57, suggesting in a different manner the foreseen deduction.

[38]Mobility Service Platform (A2.3), EH Web server (A1.5) and Customer data (A0.1).

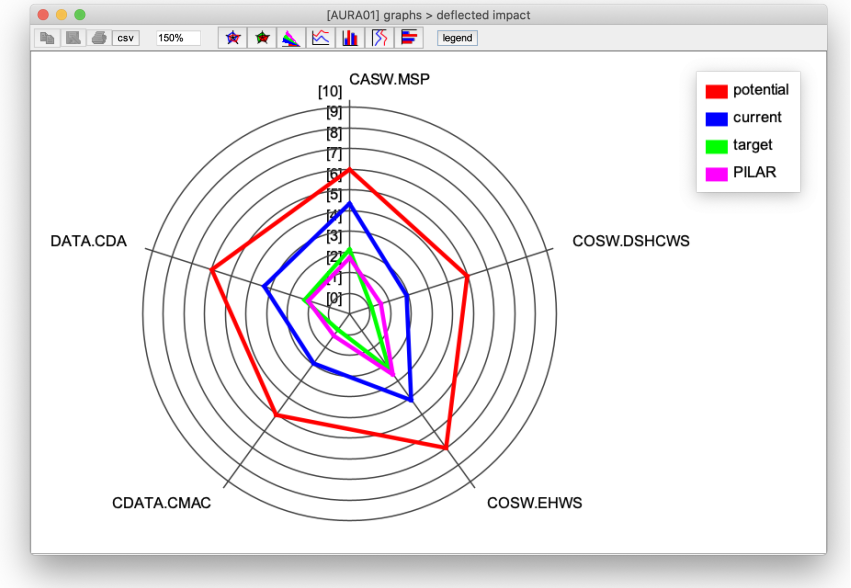


Figure 56: Deflected Impact Comparison B in Pilar

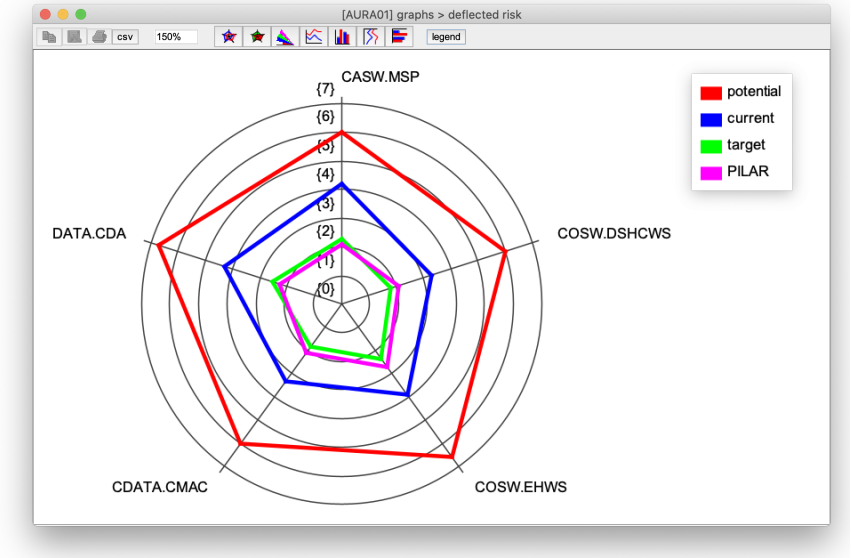


Figure 57: Deflected Risk Comparison B in Pilar

7.4.4 Security Profiles (E)

This last section of the demo performed in Pilar provides an overview about the compliance of our case study with the security profiles[39] that we had included in the project:

- "Code of practice for information security controls" [MAGERIT - ISO/IEC 27002:2013]
- "Regulation on the protection of natural persons with regard to the processing of personal data" [MAGERIT - GDPR:2016]
- "Code of practice for personally identifiable information protection" [MAGERIT - ISO/IEC 29151:2017]

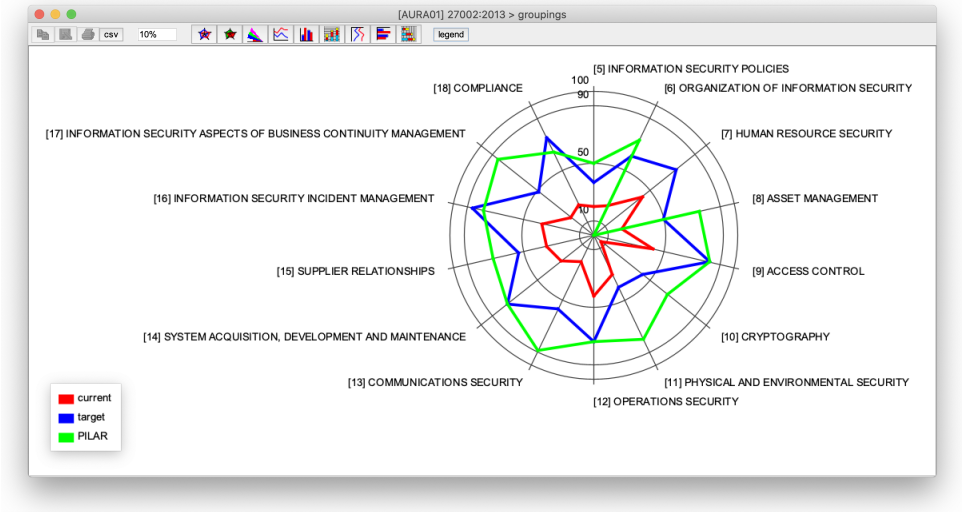


Figure 58: ISO/IEC 27002:2013 Compliance in Pilar

By proceeding in order, we can observe the ISO/IEC 27002:2013 compliance values in Fig.58 with a comparison between the three phases. As the red line illustrates, the current phase seems to be quite disastrous especially

[39] We already performed the assessment of the three security profiles in Sec.7.4.2.

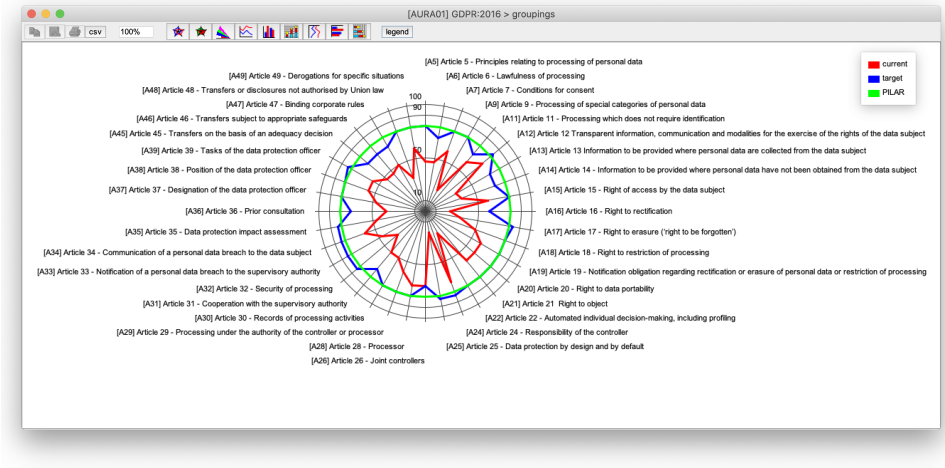


Figure 59: GDPR Compliance in Pilar

for the following items: asset management [8], cryptography [10], communication security [13], information security aspects of business continuity management[17]. As a result in addiction to technical measures and protections to minimise impacts and risks, several compliance measures should be implemented in order to reach the target phase. As the figure depicts, the latter aims to prioritise the following items: human resource security [7], access control [9], information security incident management [16] compliance [18].

Generally personal data should be considered a critical point — for instance this was confirmed by the assessment of the Customer data (A0.1). Regarding GDPR compliance, here the situation results quite heterogeneous, as illustrated in Fig.59. In the current phase we can identify some of the most critical items, among others: Article 16 - Right to rectification [A16], Article 17 - Right to erasure ('right to be forgotten') [A17], Article 22 - Individual decision-making, including profiling [A22], Article 25 - Data protection by design and by default [A25], Article 32 - Security of processing [A32]. In particular, articles 17, 25 and 32 should be prioritised as well.

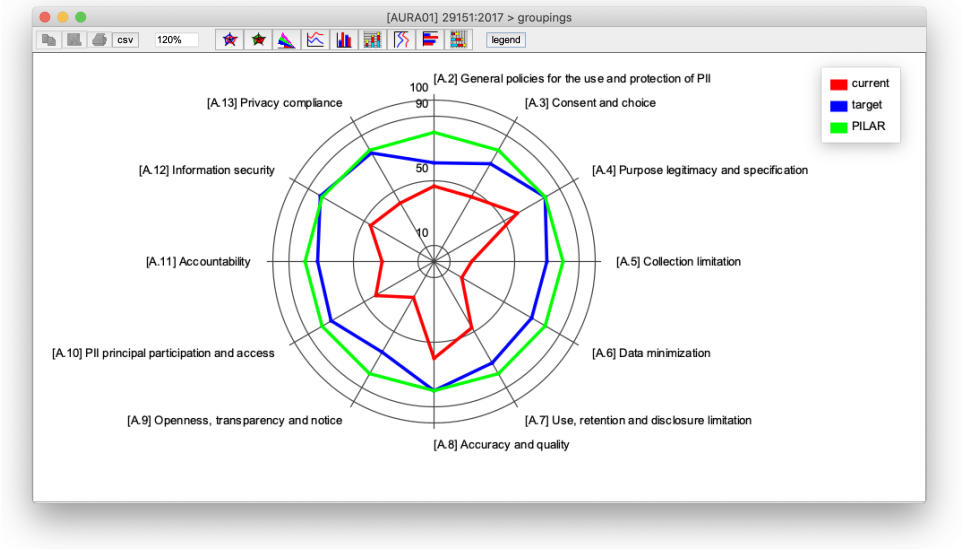


Figure 60: ISO/IEC 29151:2017 Compliance in Pilar

Eventually we can conclude this case study report by analysing the compliance with ISO/IEC 29151:2017, shown in Fig.60. In the case of the personally identifiable information (PII) compliance, the current phase mostly appears to suffer in the following items: Collection limitation [A.5], Data minimisation [A.6], Openness, transparency and notice [A.9], Accountability [A.11].

In conclusion, all of the three analyses of the security profiles have emphasised the importance of the compliance with regulations and international standards, as a negligence[40] in some of the items might affect assets and, consequently, their impact and risk values.

[40]Impact and risk values of the Customer data (A0.1) asset is influenced by GDPR and ISO/IEC 29151:2017 compliance in the current phase.

8 Conclusions

The main goal of a Risk Assessment process consists in bringing to light concealed risks and/or confirming most of the weaknesses (e.g., vulnerabilities, lack of compliance, etc.) in the organisation. It is also important to remember that RA is a cyclic process, and it would be significantly simplified if the organisation followed what we can refer as "cybersecurity best practices", such as security by design and privacy by design. From the results derived from the analysis carried out on the proposed case study, the critical issues regarding the automotive sector introduced in the previous sections have been confirmed. In particular, we were able to ascertain that, on the basis of a plausible example, and the state of the art technology in the automotive sector, Risk Assessment has allowed us to understand the components most at risk: communication peripherals and cloud. Finally, it should be noted that both may potential threaten personal data, which are increasingly protagonists in the exchange of information between V2X communication platforms.

The MAGERIT methodology has proved to be a general methodology that can also be applied to a specific scenario, such as the case study proposed in Sec.7 in the automotive field. A further point in its favor is certainly compliance with the ISO/IEC 27005 standard, among others, as well as the useful possibility to integrate it with the use of any threat modeling, such as STRIDE.

As far as the applicability of the methodology is concerned, the PILAR tool certainly represents an added value which, however, has its drawbacks. Despite on the one hand Pilar is maintained up to date, within the add of complete and huge libraries (i.e., GDPR compliance, threats list, assets categories, etc.) which help and simplify[41] the identification phases, although

[41] In the sense that it is difficult for us to miss something because it is practically all included.

on the other hand the tool[42] results often repetitive and confusing in some stages. A final sore point concerns the algorithms implemented in Pilar: being a commercial software, it is not possible to understand precisely how the tool calculates the values — unless trying to approximate by empirical experiments, such as our proposal in Sec.6. In other words, we should have faith in the correct implementation of the algorithms.

8.1 Future work

Further in-depth analysis of the algorithms implemented in Pilar (i.e., improved mathematical fits, reverse engineering) would be a good starting point for a future improvement of the presented study. Moreover, we observed that the tool does not offer support for Risk Treatment, thereby we could leave this process to be employed in a future work, as well as Risk Acceptance, to conclude the first cycle of the Risk Management process for the case study analysed.

It would be relevant to extend this analysis within the integration of a Data Protection Impact Assessment (DPIA) process[39], to analyse, identify and minimise the data protection risks of the case study. In addiction, another point to extend could be the add of other smart car features, like autopilot, Machine Learning (ML) and Artificial Intelligence (AI) components for semi-autonomous and autonomous cars, and so on.

Eventually, it would also be relevant to repeat the same experiment using other methodologies (and tools) — comparing them with Magerit (and Pilar) — to better understand which one would (quasi-)perfectly suit the field of automotive.

[42]The basic version at least. There exists a "micro" version which claims to be more efficient and fast (no evaluation licenses, paid only).

References

[1] EU, *General Data Protection Regulation (GDPR)*, May 04, 2016.
https://eur-lex.europa.eu/eli/reg/2016/679/oj

[2] EU, *European Union Agency for Cybersecurity (ENISA)*.
https://www.enisa.europa.eu/

[3] ISO/IEC 27005, *Information technology — Security techniques — Information security risk management*, July, 2018.
https://www.iso.org/standard/75281.html

[4] NIST, *SP 800-30*, January 16, 2020.
https://www.nist.gov/privacy-framework/nist-sp-800-30

[5] ENISA, *CRAMM Method*.
https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_cramm.html

[6] ANSII, *EBIOS Method*.
https://www.ssi.gouv.fr/guide/ebios-risk-manager-the-method/

[7] ENISA, *MEHARI Methodolody*.
https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_mehari.html

[8] EAR/PILAR, *MAGERIT Methodolody*, July, 2014.
https://www.pilar-tools.com/magerit/index.html

[9] OWASP, *Risk Assessment Framework*.
https://owasp.org/www-project-risk-assessment-framework/

[10] ISF, *Standard of Good Practice for Information Security*, 2020.
https://www.securityforum.org/tool/
standard-of-good-practice-for-information-security-2020/

[11] IEEE Spectrum, Robert N. Charette *This Car Runs on Code*, February 01, 2009.
http://spectrum.ieee.org/transportation/systems/
this-car-runs-on-code

[12] IEEE, Jonathan Petit, Steven E. Shladover *Potential Cyberattacks on Automated Vehicles*, September 06, 2014.
https://ieeexplore.ieee.org/document/6899663

[13] ENISA, *Risk Management*.
https://www.enisa.europa.eu/topics/
threat-risk-management/risk-management/current-risk/
risk-management-inventory/introduction

[14] ENISA, *Risk Management Glossary*.
https://www.enisa.europa.eu/topics/
threat-risk-management/risk-management/current-risk/
risk-management-inventory/glossary/

[15] ENISA, *Risk Assessment*.
https://www.enisa.europa.eu/topics/
threat-risk-management/risk-management/current-risk/
risk-management-inventory/rm-process/risk-assessment

[16] ISO/IEC 27001, *Information Security Management*, 2013.
https://www.iso.org/isoiec-27001-information-security.
html

[17] Wikipedia, *Threat Model*.
https://en.wikipedia.org/wiki/Threat_model

[18] ThreatModeler, *Threat Modeling Methodologies*.
https://threatmodeler.com/threat-modeling-methodologies/

[19] Microsoft, *STRIDE Threat Model*, November 12, 2009.
https://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx

[20] ISO/IEC 31000, *Risk Management*, 2018.
https://www.iso.org/iso-31000-risk-management.html

[21] MAGERIT, *Book I: The Method*, July, 2014.
https://www.pilar-tools.com/magerit/index.html

[22] MAGERIT, *Book II: Catalogue of Elements*, October, 2012.
https://www.pilar-tools.com/doc/magerit/2012_Magerit_v3_libro2_catalogo%20de%20elementos_es_NIPO_630-12-171-8.pdf

[23] MAGERIT, *Book III: Practical Techniques*, October, 2012.
https://www.pilar-tools.com/doc/magerit/2012_Magerit_v3_libro3_guia%20de%20tecnicas_es_NIPO_630-12-171-8.pdf

[24] MAGERIT, *Magerit vs. ISO 27005*.
https://www.pilar-tools.com/doc/magerit.pdf

[25] PILAR, *Documentation*, July, 2014.
https://www.pilar-tools.com/en/tools/pilar/v74/doc.html

[26] PILAR, *Risk Analysis in Pilar*.
https://www.pilar-tools.com/doc/ISO27005.pdf

[27] PILAR, *Glossary of Terms*.
https://www.pilar-tools.com/en/glossary/index.html

[28] Wikipedia, *Regression Analysis*.
https://en.wikipedia.org/wiki/Regression_analysis

[29] Wikipedia, *Vehicle-to-Everything*.
https://en.wikipedia.org/wiki/Vehicle-to-everything

[30] ZDNET, *What is V2X communication? Creating connectivity for the autonomous car era*, November 04, 2019.
https://tiny.cc/ZDNET-V2X-Connectivity

[31] Wikipedia, *Automotive Security*.
https://en.wikipedia.org/wiki/Automotive_security

[32] Black Hat USA 2020, *Security Research on Mercedes-Benz: From Hardware to Car Control*, August 06, 2020.
https://tiny.cc/BH20-Mercedes-Security

[33] Kaspersky, *Black Hat USA 2015: The full story of how that Jeep was hacked*, August 06, 2015.
https://www.kaspersky.com/blog/
blackhat-jeep-cherokee-hack-explained/9493/

[34] STRIVE 2019, *CANDY CREAM: haCking infotAiNment AnDroid sYstems to Command instRument clustEr via cAn data fraMe*, December 05, 2019.
https://ieeexplore.ieee.org/document/8919510

[35] Ward, Ibarra, Ruddle, *Threat Analysis and Risk Assessment in Automotive Cyber Security*, April 08, 2013.
https://doi.org/10.4271/2013-01-1415

[36] Toyota, *Connected Vehicles*, June 26, 2018.
https://global.toyota/en/newsroom/corporate/23157821.
html

[37] Macher, Armengauda, Brennerb, Kreiner, *Threat and Risk Assessment Methodologies in the Automotive Domain*, 2016.
https://doi.org/10.1016/j.procs.2016.04.268

[38] Automotive Linux Summit, Lin Tong, Chen Luhai, *Common Attacks Against Car Infotainment Systems*, July, 2019.
https://tiny.cc/ALS19-Attacks-IVI

[39] EU, GDPR, *Data Protection Impact Assessment (DPIA)*.
https://gdpr.eu/data-protection-impact-assessment-template/