

D4.5 FRACTAL Security Capabilities

Deliverable Id:	D4.5
Deliverable name:	FRACTAL Security Capabilities
Status:	Draft
Dissemination level:	Public
Due date of deliverable:	2022-10-31 (M26)
Actual submission date:	2022-10-26
Work package:	WP4 "Safety, Security & Low Power Techniques"
Organization name of lead contractor for this deliverable:	IKER
Authors:	Christian Martín, IKER Mariana García, IKER Alfonso González, ZYLK Rubén Naranjo, ZYLK Iñigo Angulo, ZYLK Silvia Gaudio, MODIS
Reviewers:	Markus Postl, VIF Ilya Tuzov, UPV

Abstract:

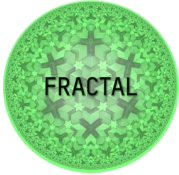
This deliverable aims to report the results and implementations of T4.4 on security capabilities for the FRACTAL node. It presents the state-of-art around cybersecurity in embedded systems. As a result of preliminary research, IoT Gateways, Risk Management and GDPR Compliance has been developed. The deliverable reports the research, development and production process of the components resulting from the completion of the task.



This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 877056

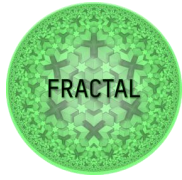


Co-funded by the Horizon 2020 Programme of the European Union under grant agreement No 877056.

	Project	FRACTAL	
	Title	FRACTAL Cybersecurity features and requirements for Fractal	
	Del. Code	D4.5	

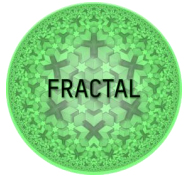
Contents

1	Historical	5
2	Summary	6
3	Introduction.....	7
4	State of Art.....	9
4.1	Cybersecurity.....	9
4.2	Cybersecurity in embedded systems	9
4.3	Containerization, isolation, networking interfaces and subnet security.....	12
4.3.1	Containerization, isolation and cybersecurity	12
4.3.2	Container networking.....	12
4.3.3	How Container networks and subnetworks are (in)secure by default	14
4.4	Cybersecurity in Edge computing & IoT networks	14
4.5	Risk Management - ISO/IEC 27005	14
4.6	STRIDE	17
5	Mitigation: IoT Gateways.....	19
5.1	What is a gateway	19
5.1.1	Gateway cybersecurity issues	20
5.1.2	A comparison between existing gateways	21
5.2	Implementation: Apache APISIX	22
5.2.1	Apache APISIX description and implementation steps	22
6	Risk Management	26
6.1	Mitigation: OS Security Layer.....	26
6.2	Context establishment	26
6.2.1	Fractal node description	26
6.2.2	Use cases	26
6.2.3	Operation context	29
6.3	Risk Assessment	29
6.3.1	Risk Identification	29
6.3.2	Risk analysis.....	33
6.3.3	Risk evaluation	38
6.4	Risk Treatment	40
6.4.1	Security Countermeasures.....	40
6.4.2	Transversal Yocto Security Layer Implementation.....	42



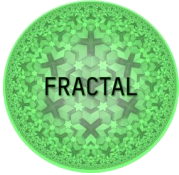
Project	FRACTAL	
Title	FRACTAL Cybersecurity features and requirements for Fractal	
Del. Code	D4.5	

6.4.3	Transversal Yocto Security Layer Verification	44
7	GDPR Compliance	46
7.1	Regulatory framework.....	46
7.2	Definitions	46
7.3	Workflow.....	47
7.3.1	Preliminary risk assessment	48
7.3.2	Define if a DPIA is needed	49
7.3.3	Method of conducting the DPIA	51
7.4	Preliminary assessment.....	52
7.4.1	Use case 1: Engineering & maintenance works.....	52
7.4.2	Use Case 2: Automotive Air Control	55
7.4.3	Use case 3: Smart meter	57
7.4.4	Use Case 4: Low-latency Object Detection as a generic building block for perception in the edge for industrial application.....	58
7.4.5	Use case 5: Increasing the safety of autonomous train through AI techniques.....	60
7.4.6	Use Case 6: Intelligent Totem – Elaborate data collected using heterogeneous technologies.....	61
7.4.7	Use case 7: Autonomous SPIDER robot	63
7.4.8	Use case 8: Shuttle for moving goods in a warehouse.....	65
7.5	Data confidentiality measures	66
7.6	Conduct the DPIA?	68
7.6.1	Use case 1: Engineering & maintenance works.....	68
7.6.2	Use case 2: AI-based control strategies (air path, thermal mgmt.) ...	69
7.6.3	Use case 3: Smart meters for everyone	69
7.6.4	Use Case 4: Low- latency Object Detection in Industry 4.0	69
7.6.5	Use case 5: Autonomous train operation	69
7.6.6	Use case 6: Intelligent totem.....	69
7.6.7	Use case 7: SPIDER autonomous robot	70
7.6.8	Use case 8: Shuttle in Warehouse Systems	70
7.7	DPIA EXECUTION	70
7.7.1	Phase 1 for all use cases	70
7.7.2	Phase 2 for use cases that require DPIA (only UC1)	71
7.7.3	Phase 2 for that do not require DPIA (UC2, UC3, UC4, UC5, UC6, UC7 and UC8).....	79



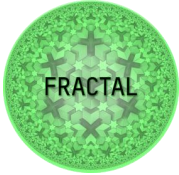
Project	FRACTAL	
Title	FRACTAL Cybersecurity features and requirements for Fractal	
Del. Code	D4.5	

7.8	DPIA results	79
7.8.1	Use case 1: Engineering & maintenance works.....	79
8	Conclusions	80
9	List of figures.....	81
10	List of tables.....	82
11	List of Abbreviations	83

	Project	FRACTAL	
	Title	FRACTAL Cybersecurity features and requirements for Fractal	
	Del. Code	D4.5	

1 Historical

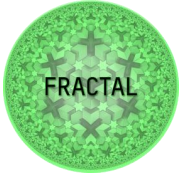
Version	Date	Modification reason	Modified by
0.1	07/02/2022	Document Created	Christian Martín
0.2	12/14/2022	MODIS added content	Marco Cappella
0.3	01/06/2022	IKERLAN Updated content	Mariana García y Christian Martín
1.0	30/09/2022	First Release	

	Project	FRACTAL	
	Title	FRACTAL Cybersecurity features and requirements for Fractal	
	Del. Code	D4.5	

2 Summary

This deliverable aims to report the outcomes of T4.4 on security capabilities. The results of the implementations carried out in the task are presented according to the components developed, which reflect the objectives of the task.

Namely, T4.4 developed security capabilities for FRACTAL systems with an IoT gateway, described in Chapter 5 (ZYLK) and a risk management approach based on ISO 27005 with the result of an OS security layer, explained in Chapter 6 (IKER). The task also performs a GDPR compliance analysis supported by a DPIA survey, reported in Chapter 7 (MODIS).

	Project	FRACTAL	
	Title	FRACTAL Cybersecurity features and requirements for Fractal	
	Del. Code	D4.5	

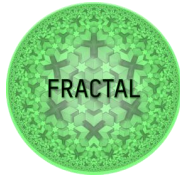
3 Introduction

The goal of the fourth work package is to develop safety, security, and low-power services for individual FRACTAL nodes. This deliverable is focused on those of security. The development of the security capabilities is transversal to all the operating system layers: IoT gateways have been developed to secure networks and endpoints within a given network, OS security layer implements the most important security countermeasures in an OS according to the standard IEC62443, and finally, the GDPR compliance follows European rules to protect personal data of a company or organization.

The Table 1 summarizes all the components developed on the Task 4.4.

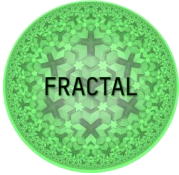
Table 1: T4.4 developed component summary

WP4T44-02 OS Security Layer	
Description	Implementation of security countermeasures in a transversal security layer
Contribution to T4.4 Objectives	Provides secure digital communications between Fractal nodes, as well as authentication and authorization schemes, complying with the IEC 62443 standard.
WP4T44-05 IoT Gateway	
Description	IoT network Gateway for external communication monitoring
Contribution to T4.4 Objectives	Single access-point for internal and external traffic into the Fractal Platform network. Security plugins can be configured for a secured environment.
WP4T44-07 Node monitoring and system status	
Description	Metrics collector for security related aspects and issue addressing
Contribution to T4.4 Objectives	Provides an overview of the system available resources. Helps preventing system resource exhaustion attacks by giving diagnostic metrics.



Project	FRACTAL	
Title	FRACTAL Cybersecurity features and requirements for Fractal	
Del. Code	D4.5	

WP4T44-08 TLS Implementation on containers	
Description	Inter-nodal secure communications. Container communications driven by TLS with secure exposed daemons.
Contribution to T4.4 Objectives	Enable TLS communications between Docker Engine daemons and containers communicate through TLS between hosts.
WP4T44-09 Runtime security	
Description	Process isolation through containerization and user control
Contribution to T4.4 Objectives	Provide a set of practices for secure container image buildings.

	Project	FRACTAL	
	Title	FRACTAL Cybersecurity features and requirements for Fractal	
	Del. Code	D4.5	

4 State of Art

4.1 Cybersecurity

The term cybersecurity means to protect information and information systems from unauthorized access and use, disclosure, interruption, modification or destruction to provide three principles: confidentiality, availability and integrity. These three principles are known as the three pillars of information security¹:

- **Confidentiality:** a system should ensure that only authorised users access information.
- **Integrity:** a system should ensure completeness, accuracy and absence of unauthorised modifications in all its components.
- **Availability:** a system should ensure that all system's components are available and operational when they are required by authorised users.

These three properties are known as the CIA Triad (Confidentiality, Integrity and Availability). Other secondary properties are accountability (responsibility), authenticity (authenticity) and non-repudiability (non-repudiation or inalienability)².

The trinity of problems is known to the three sources of vulnerability:

- **Complexity:** current software is complex and insecure languages such as C and C++ are used. This increases the likelihood of bugs and vulnerabilities. Some examples of simple attacks are buffer-overflows or dangling pointer errors.
- **Extensibility:** current software is not static but is constantly evolving. Updates and bug fixes can eliminate existing vulnerabilities but open others at the same time. On the other hand, dynamic loads of drivers and modules can affect the vulnerability of the system.
- **Connectivity and remote use of embedded devices:** this can lead to network-induced vulnerabilities (for example, remote attacks and fault propagation between peer devices).


In the case of embedded systems there is a fourth factor which is the operation in an unreliable environment (untrusted) in which someone can take control of the system physically.

4.2 Cybersecurity in embedded systems

The main difference between the security of IT systems and of embedded systems is that in the case of embedded systems, in addition to remote attacks, there may be physical attacks (that is, side-channel attacks, reverse engineering, device

¹ <https://www.nccoe.nist.gov/publication/1800-25/VolA/index.html>

² <https://users.cs.cf.ac.uk/Y.V.Cherdantseva/RMIAS.pdf>

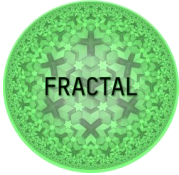
	Project	FRACTAL	
	Title	FRACTAL Cybersecurity features and requirements for Fractal	
	Del. Code	D4.5	

tampering, etc.). A physical attack would suppose the total control of the system with its serious consequences.

Note that latter chapters do not handle those type of attacks. This is due to the diverse hardware architecture of potential FRACTAL users. However, in addition to mitigation at the operating system and network level, the user must apply environmental and physical security measures according to their platform. In embedded systems, attacks can be directed at the design of an embedded system (abstract model) or at the actual device, then at its implementation. In most cases the real device is attacked.

A classification of attacks on embedded systems, as also shown in the Figure 1, can be:

- 1) **Functional:** affecting the functioning of the system and attacking the main security properties: integrity (hash functions as a security mechanism), confidentiality/privacy (through encrypted algorithms) and availability.
- 2) **Based on agents:** which refer to the media or agents that cause the attack and define the types of attacks: eavesdropping, microprobing, power analysis, fault injection, virus, man-in-the-middle, etc. These are classified into three categories:
 - **Software attacks:** for example, viruses, worms or Trojans that can misconfigure or create buffer-overflows. These attacks are less expensive than physical ones.
 - **Side-channel attacks:** use of certain underlying information such as consumption, electromagnetic waves to deduce patterns.
 - **Physical attacks:** they directly access the device (chip, memory, etc.). For example, a microprobing attack (accessing the surface of the chip) or eavesdropping (interception of communication).

	Project	FRACTAL	
	Title	FRACTAL Cybersecurity features and requirements for Fractal	
	Del. Code	D4.5	

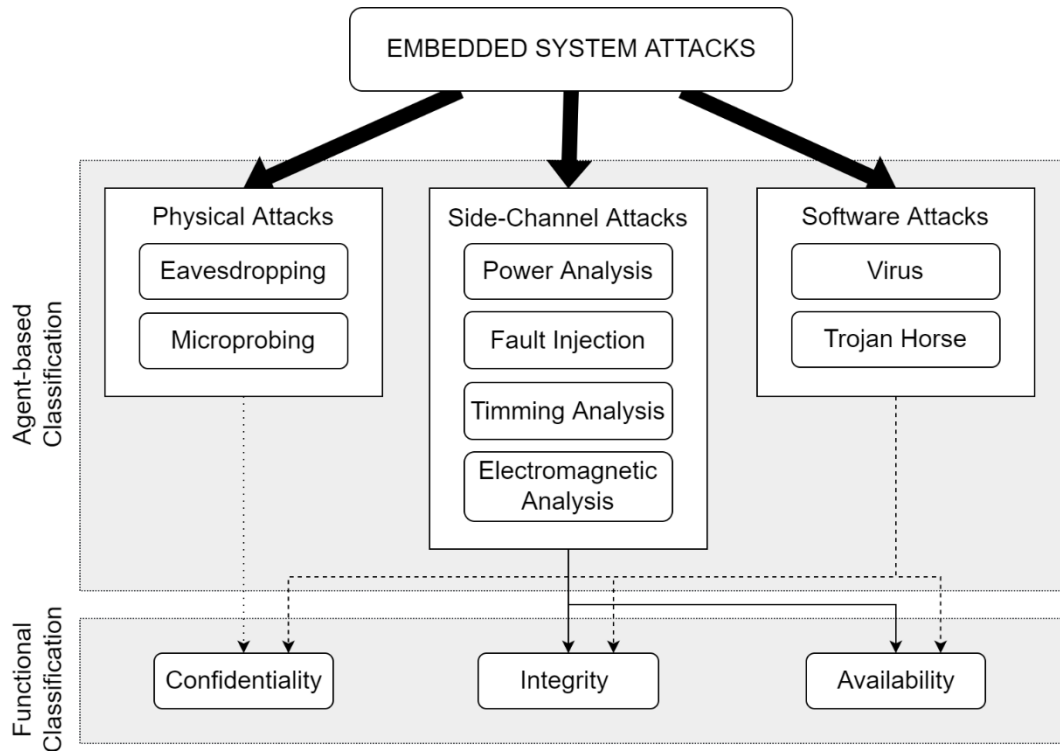


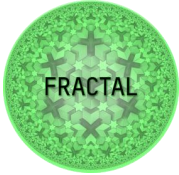
Figure 1: Attacks on embedded systems

The following points show the difficulty of addressing the security problem in embedded systems.

- **Processing:** there is difficulty in meeting the computational needs for security processing.
- **Battery:** power consumption for security processing can be high.
- **Flexibility:** sometimes security can involve the execution of various security protocols and standards.
- **Tamper resistance:** embedded systems can be attacked by a large number of attacks at the software (for example, viruses or Trojans) and hardware level.
- **Assurance:** related to reliability and indicates the fact that the system must function independently of attacks.
- **Cost:** the cost of the embedded system will be higher by integrating security measures along with the fact that a better processor or an additional chip is still needed.

The following points show the existing challenges when it comes to achieving embedded security:

- **Software maintenance:** so that updates are safe.
- **Theft prevention:** the idea is to restrict the use of the system. A widely used mechanism is the 'electronic immobilizer', such as a car remote control key to open a car and start it. The security applications used are usually related to the biometric area.

	Project	FRACTAL	
	Title	FRACTAL Cybersecurity features and requirements for Fractal	
	Del. Code	D4.5	

- **Access control**
- **Support for new business models:** fundamentally referred to embedded devices that use certain content to show the consumer. Then the legal rights of the owner should be protected.
- **Personalization/identification:** by identifying a user, the actions performed on the device can be saved
- **Legal obligations:** there are applications to achieve compliance with the law (charging systems on the roads or the tachometer). Tampering with these systems should not be allowed.

4.3 Containerization, isolation, networking interfaces and subnet security

Containerization is becoming one of the most popular ways of software virtualization. During the last years, containers have been used over other virtualization techniques as Virtual Machines, because they have a smaller footprint, do not require a heavy configuration and are simple to deploy over multiple cloud and edge environments. The results of the investigation over secure approaches on containerization technologies are reflected on the following components: Runtime security, Node monitoring and system status and TLS Implementation on containers (WP4T44-09 , WP4T44-08 , WP4T44-07).

4.3.1 Containerization, isolation and cybersecurity

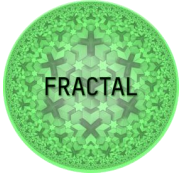
The main feature of containers in terms of security is isolation. Docker containers, for instance, use the isolation capabilities of Linux systems (mainly cgroups and namespaces) to be run in a completely isolated manner, so the host system is totally unaware of the processes being run inside the virtual environment.

Their black-boxed functionality makes containers secure by design, but processes running completely isolated are of course completely useless. Data exchange and storage, user interaction and task offloading are required from containers, and this is the open gate for security threats and vulnerabilities. A completely isolated container running a threatening process will never be a risk for the host machine or other systems, but this is rarely the case. Ultimately, processes run in the container serve a purpose, and the data or resources generated from such processes end up being used by other systems.

These data exchange and external interaction features are provided by two mechanisms: (1) Networking interfaces and (2) filesystem mounts or volumes.

4.3.2 Container networking

There is a clear difference between a container and the physical hardware running it, however, operationally they are not distinguishable in terms of networking. Containers are enabled to communicate with other containers, their host, and share their resources and applications, exactly as any physical node does. For this reason,

	Project	FRACTAL	
	Title	FRACTAL Cybersecurity features and requirements for Fractal	
	Del. Code	D4.5	

containers are subject to every intrinsic security threat related to being connected to a network.

Container networking, however, follows slightly different approaches than classical networks, because containers usually do not need to communicate with external devices apart from their own host. For example, a database being stored in a container will only communicate with its host, which could be running an application exposed to other systems, and in this case, there is no need to connect the container to the external network. For this reason, containers can be run in their own network namespace, instead of their whole host network.

These characteristics brought the definition of two networking standards for containers, the Container Network Model from Docker and the Container Network Interface by CoreOS:

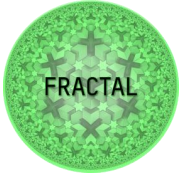
- *Container Network Model (Docker)*

There are several ways to connect containers and hosts within each other, through the following network types:

- **None:** The container has no IP and is unable to communicate with any other system. This network mode is mostly used for container testing or for containers which don't need external communication.
- **Bridge:** This network mode allows connections to other interfaces within the host. By default, scheduled containers are connected to the bridge network, and open ports in the container can be accessed by external applications.
- **Host:** The host network mode is similar to the bridge, but uses directly the host's ports to expose applications being run inside the container. The ports in the container are bound to the host's ports, so special attention should be paid to this when containers are scaled because port conflicting is very likely to happen when dealing with thousands of containers in the same host. An external application accessing the host's ports is unable to know if the responding process behind the port is being run on a container or the host itself.
- **Overlay:** Overlay networks use tunnels to communicate between hosts running containerized applications distributedly. Containers running in different hosts will be connected to their own host's bridge networks, and would be unable to communicate with each other. Overlaying the hosts within the same network solves this problem and allows inter and intra nodal communications.

- *Container Network Interface (CoreOS):*

In this specification, the CNI is a simple contract between the container runtime and a network plugin, allowing multiple plugins to be run at the same time, depending on the use case's requirements in terms of networking.

	Project	FRACTAL	
	Title	FRACTAL Cybersecurity features and requirements for Fractal	
	Del. Code	D4.5	

4.3.3 How Container networks and subnetworks are (in)secure by default

As mentioned, these networking approaches make container networks secure, but only as long as they are not exposed to the outside world. A containerized application is indistinguishable from a bare metal or VM application, so they are still vulnerable to most common networking attacks like BotnetC2, crypto jacking, denial of service and ransomware. Container-specific firewall rules can be applied together with micro segmentation strategies to mitigate these vulnerabilities, which combined with securely designed APIs, can make exposing containerized applications secure enough.

4.4 Cybersecurity in Edge computing & IoT networks

Security mechanisms in classical cloud architectures typically consist of additional software running on the systems, making sure that the information and connections going inside or outside the system are trustworthy, while analyzing all the information packages transmitted. These security software stacks add a process overhead and take resources from the system, while edge devices with low power restrictions and limited computational capabilities are unable to run them due to their limited resources, which makes cybersecurity in edge architectures a challenge.

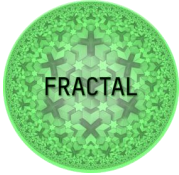
Take as an example the two main key management strategies for data privacy, which are distributed symmetric encryption keys, and public key infrastructure. None of these approaches are appropriate for IoT systems, the first one, because each of the devices must store a key for each device it has to communicate with, and this is not scalable when the number of IoT devices increases. The latter one is not suitable either because of the aforementioned constrained computational capabilities. In addition to this, edge devices are usually exposed to physical attacks, which makes it necessary to implement physical attacks protection systems, like tampering devices or port blockers.

Leaving aside physical attacks, the solution for an overall secure edge architecture is non-trivial, and the approach in Fractal, where nodes are dynamically grouped and decoupled to join their computational workforce, should be addressing the network *from the outside* rather than *from the inside*. A proposal for this could be implementing an IoT gateway system, which would act as an incoming gate for all external traffic coming into the Fractal network, and make the communications inside the network secure by distributing and controlling external traffic into secure endpoints.

4.5 Risk Management - ISO/IEC 27005

The security risk management process is based on ISO/IEC 27005³. It is a systematic establishment, assessment and treatment process of all risks associated and/or

³ ISO/IEC 27005 - Information technology — Security techniques — Information security risk management, <https://www.iso.org/standard/75281.html>

	Project	FRACTAL	
	Title	FRACTAL Cybersecurity features and requirements for Fractal	
	Del. Code	D4.5	

related to a given scenario or purpose. The risk assessment process, in turn, includes identification, analysis and evaluation stages, as shown in Figure 2.

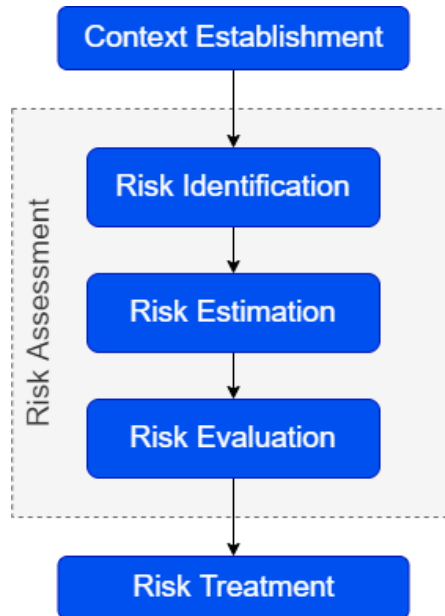


Figure 2: Information security risk management based on ISO/IEC 27005:2018

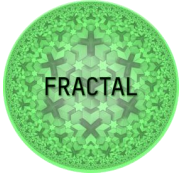
Context Establishment is needed to determine the environment and conditions in which the risk assessment takes place.

Risk assessment process plays an important role in the cybersecurity management processes, since the identification and qualification of the security threats and risks is essential when it comes to the protection of assets. This task and responsibility shall be jointly addressed by all actors/entities involved in the cybersecurity management process of the system under consideration. For this purpose, the following activities are performed:

- Identification of the assets (elements) involved in the analysis, their relationship and value with the aim of estimating possible consequences.
- Identification of security threats that assets are exposed to.
- Identification of already adopted and/or implemented safeguards that aim at protecting the assets.
- Determination and evaluation of risks based on the potential impacts in face of an attack and the likelihood of such attack.

The technical document IEC 62443-4-1⁴ defines the cybersecurity-related lifecycle development requirements for IACS and provides guidance on how to meet the described requirements. Specifically, in Practice 2 (Specification of security

⁴ IEC 62443-4-1:2018 - Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements, <https://webstore.iec.ch/publication/33615>

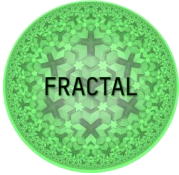
	Project	FRACTAL	
	Title	FRACTAL Cybersecurity features and requirements for Fractal	
	Del. Code	D4.5	

requirements), requirement SR-2 (Threat Model), establishes the need to address product cybersecurity based on the definition of a threat model that allows an orderly analysis of the cybersecurity features of the product.

The threat model is therefore a risk assessment in the classical context of information security adapted to the industrial environment and which is of vital importance to correctly protect a component.

From the risk assessment results, will be generated a risk treatment. Risk Treatment is the process of selecting and implementing of measures to modify risk. Risk treatment measures can include avoiding, optimizing, transferring or retaining risk⁵. It will be a good part of the cybersecurity requirements to be met / developed in the product.

⁵ <https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-process/risk-treatment>

	Project	FRACTAL	
	Title	FRACTAL Cybersecurity features and requirements for Fractal	
	Del. Code	D4.5	

4.6 STRIDE

STRIDE⁶ is a methodology created by Microsoft to identify threats related to security, more specifically computer security. Table 2 details the properties necessary to counter STRIDE threats.

Table 2: Desired properties related to the STRIDE threats

Threat	Desired Property
Spoofing	Authenticity
Tampering	Integrity
Repudiation	Non-repudiability
Information disclosure	Confidentiality
Denial of Service	Availability
Elevation of Privilege	Authorization

In this methodology, every item in a system is evaluated as an external entity, a process, data store or data flow, as shown in the Figure 3. In addition, each type of element has its unique type of vulnerabilities associated, as shown in the Figure 4. That vulnerabilities need to be assessed and solved.

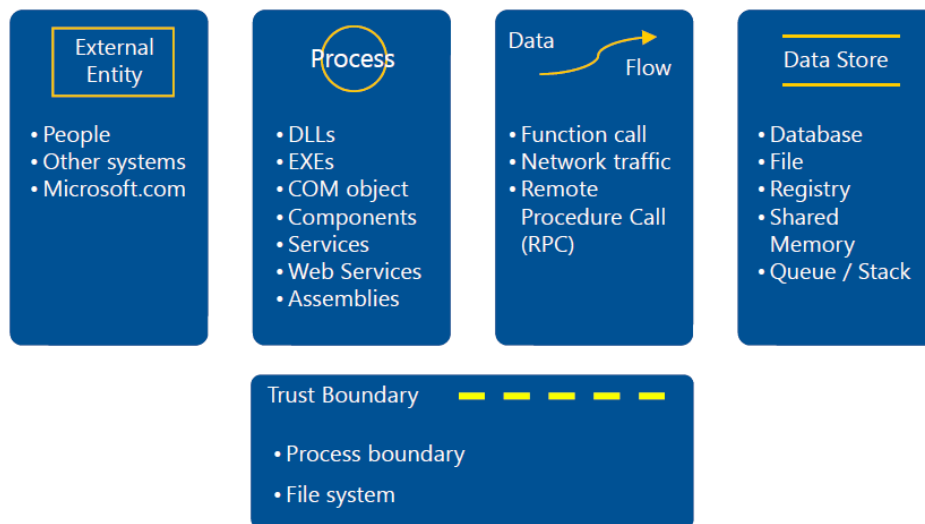
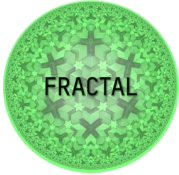


Figure 3: Elements in the STRIDE methodology

⁶ The STRIDE Threat Model, Microsoft, [https://docs.microsoft.com/en-us/previous-versions/commerce-server/ee823878\(v=cs.20\)](https://docs.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20))

	Project	FRACTAL	
	Title	FRACTAL Cybersecurity features and requirements for Fractal	
	Del. Code	D4.5	






ELEMENT	S	T	R	I	D	E
 External Entity	✓		✓			
 Process	✓	✓	✓	✓	✓	✓
 Data Store		✓	?	✓	✓	
 Data Flow		✓		✓	✓	

Figure 4: Type of vulnerabilities according to the STRIDE methodology

	Project	FRACTAL	
	Title	FRACTAL Cybersecurity features and requirements for Fractal	
	Del. Code	D4.5	

5 Mitigation: IoT Gateways

With the growth of microservices based architectures, API based communications are becoming very common nowadays. For this, API management layers and tools are gaining importance, as in the case of API gateways. An API gateway offers a single and unified API entry point across several internal APIs. Thus, this component is often used as the access point for the incoming and outgoing communications within a particular subnet or environment. Moreover, API gateways can provide many security mechanisms, such as different strategies for user authentication and authorization, traffic control, etc.

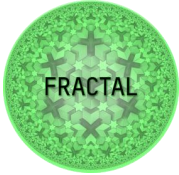
As mentioned, APIs (and in recent years, APIs based on REST design principles specially) are mechanisms to enable microservice interaction inside an application's private network, but microservices must be finally exposed to the end users and the exterior. These architectures are not scalable, because thousands of microservices being exposed at different endpoints highly increase the application's attack surface and compromise the whole network security. Especially in edge deployments, where there could be from hundreds to thousands of devices each running their own applications. As the edge must provide a way to manage a wide range of microservices, while also ensuring secure endpoint exposure, API gateways are a key component in edge architecture designs.

At the present, there exist many API gateway products, and there is a variety of options for particular situations and designs. In this section, we present some of these tools, a comparison between them, and some thoughts regarding their applicability on the Fractal ecosystem.

5.1 What is a gateway

Endpoints are addresses exposed by any application running inside a host machine. These endpoints are the entry for communicating with the applications, and as such, they are the first focus for attackers and malicious software trying to exploit vulnerabilities or buggy software. Malicious interactions with exposed endpoints on a network are a compromise in security, because even while running in containerized environments, privilege escalation attacks can be used to gain control of the host machine. Securing endpoints is the process of making the interactions between external users (and potential attackers) with the application secure, and it can be achieved through several methods, defining rule sets and analyzing each of the endpoint's potential exploitation vulnerabilities. However, when dealing with edge networks that can be formed by thousands of endpoints, communicating with each other, a thorough analysis of each of the endpoints is not viable. This is why a secure way of accessing the network and its resources must be found, and where gateways become an applicable resource.

A gateway consists of a data communication system, either being hardware or software (or a combination of both) that enables data flow from one network to

	Project	FRACTAL	
	Title	FRACTAL Cybersecurity features and requirements for Fractal	
	Del. Code	D4.5	

others. It can operate on the seven layers of the OSI model and allows communication between different protocols. Typically, a network gateway connects a home or office local area network (LAN) to the Internet. Gateways become especially relevant in the IoT field, where the network gateway also acts as a protocol converter between light-weight devices and microservices, allowing the IoT devices to keep low communication thresholds and saving resources.

Gateways are usually the single-entry point to a network, so external users, sessions, and the whole in-and-out traffic only have one entrance into the network. Input traffic to specific resources inside the network is then redirected into the different components and devices (and their respective endpoints). This is how a gateway helps securing a network; by having a single-entry point for all external traffic, it can be monitored in a simple and centralized way. Moreover, gateways usually have the ability to establish different policies for each kind of exposed device or microservice or even for different internet traffic patterns, enabling user authentication, IP restriction, load balancing, etc. This layer ensures that the users and applications accessing the gateway and the network resources have trusted identities, protecting devices from intrusions, and protecting the data integrity.

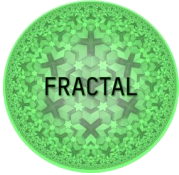
Gateways cannot only be used for Internet traffic control, but they have a wide applicability to all kinds of computing architectures. For instance, they are a key part of hybrid cloud-edge architectures, where they allow for device-to-cloud communications and translation between cloud and edge communication protocols. They can also perform other kinds of tasks, like data-aggregation, local processing of data and local data storage. These pre-processing capabilities allow edge devices to save on computing resources, providing an indirect protection against resource -exhausting attacks on IoT devices.

5.1.1 Gateway cybersecurity issues

As mentioned, gateways are used to secure networks and all the endpoints within a given network, so that they cannot be accessed directly. This makes the gateway itself the main focus for attackers, as being able to manipulate and control the gateway would give total control to the external attacker. Several bots for denial-of-service attacks have been used in the past (Mirai attack) to get control of gateways, even though the malicious devices performing the DoS attack were internally infected devices.

The goal of network security and in this case of the IoT Gateway is always to prevent the breaching of the network by stopping an attack before it has compromised any device or service on the network. Unfortunately, that is not always the case as attackers may find ways to circumvent the discussed security measures, be it by finding bugs or discovering another way to elude the implemented security policies. Thus, it is critical to assess the risks that an attack can have over the network and implement mechanisms to mitigate the possible damage.

If a network is already compromised, there are a handful of options for the attacker to take as next steps:

	Project	FRACTAL	
	Title	FRACTAL Cybersecurity features and requirements for Fractal	
	Del. Code	D4.5	

- Disable a device or service: One of the most common attacks a device can suffer is the Denial of Service (DoS), where the attacker generates so much traffic going into the device that it overwhelms its capabilities and disables the service provided by this device. This attack is especially relevant in IoT environments, since IoT devices being designed to consume as little as possible power, withstand large data flow worse than conventional PCs.
- Destroy a device: Some attacks may cause the permanent destruction of a device. For example, some IoT devices run on batteries, and an attack could raise battery usage to the point of exhaustion or raise general usage to increase temperature to the point of malfunction.
- Launch attacks: An infected device could be used as a launch point for more attacks in the network since it (potentially) has access to other elements on the network.
- Include the device into a botnet: The infected device could be added to a botnet to perform coordinated DDoS (Distributed DoS) attacks. Effectiveness of this method was proven in 2017 with Mirai (whose source code has been released) and its ability to manage 300K+ devices easily.

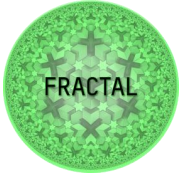
5.1.2 A comparison between existing gateways

In the following table⁷ a comparison between the most popular API gateways is shown. Several aspects and features are compared which can help decide what API gateway best suits the necessities of each scenario.

Table 3: API Gateways comparison

API gateway	Kong	APISIX	Trk	Apigee	AWS Gateway	Aliyun Gateway
Deployment patterns	stand-alone	stand-alone	stand-alone	Single machine not supported	PaaS	PaaS
Data is stored	Postgres 8or Cassandra	etcd	Redis	Postgres, Cassandra and Zookeeper	PaaS	PaaS
Whether open source	Yes, The Apache 2.0 protocol	Yes, The Apache 2.0 protocol	Yes, MPL protocol	no	no	no
The core technology	Nginx+Lua	Nginx+Lua	Golang	Unknown	Unknown	Unknown
Private deployment	yes	yes	yes	no	no	no

⁷Gateway comparison <https://www.mo4tech.com/how-to-choose-the-right-microservices-api-gateway-for-you-compare-kong-apisix-trk-apigee-and-other-gateways.html>

	Project	FRACTAL	
	Title	FRACTAL Cybersecurity features and requirements for Fractal	
	Del. Code	D4.5	

API gateway	Kong	APISIX	Trk	Apigee	AWS Gateway	Aliyun Gateway
Custom plug-in	yes	yes	yes	no	no	no
Community activity	high	high	high	In the	low	low
Connects to the external IdP	no	yes	no	yes	yes	no
Support yaml	yes	yes	no	no	no	no

- PaaS (Platform as a Service) is a cloud computing model that provides customers a complete cloud platform—hardware, software, and infrastructure—for running applications without the need of building and maintaining that platform on-premises.

As the Fractal ecosystem is mainly based on open-source tools, only open-source API gateways are considered. Furthermore, the Fractal software stack is aligned with the use of containers and orchestrators, so the existence of Docker images for these tools was another point to take into account. With these ideas in mind, we focused on Apache Apisix and Kong products, which both have Docker images for x86 and ARM64 architectures. Any of these tools would be suitable for the Fractal environment.

Further research⁹ shows that, even though both tools are high performing, Apisix seems to be over Kong in terms of Latency, MQTT support and other transcoding such as gRPC. Moreover, Apisix has a dedicated dashboard which can be very useful to facilitate user configuration and maintenance of the tool.

For these reasons and for demo purposes, we focused on Apache Apisix as the API gateway component. The following section focuses on giving an overview of the functionalities it can offer for the Fractal ecosystem.

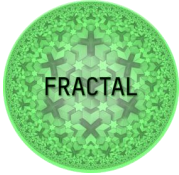
5.2 Implementation: Apache APISIX

5.2.1 Apache APISIX description and implementation steps

Apache APISIX¹⁰ operation principle is as follows; First of all, Apisix is deployed as a service. This service could be directly deployed on a machine over an OS, or also via an orchestrator engine using the available Docker images for the service. Deployment location and networking configuration are important points to keep in mind in order to get the expected operation from the tool. Here, pre-existing network infrastructure has to be inspected to ensure environment segmentation/isolation (when using orchestration tools, this is also related to particular network "driver modes" configuration). This is important due to the fact that the API gateway could be used in different situations, such as in cloud environments, for securing edge servers or even for controlling access to a group of Fractal nodes. For this reason, it is helpful to analyze the environment beforehand, to get a better idea on system requirements,

⁹ <https://api7.ai/blog/api-gateways-apache-apisix-and-kong-selection-comparison>

¹⁰ <https://apisix.apache.org/>

	Project	FRACTAL	
	Title	FRACTAL Cybersecurity features and requirements for Fractal	
	Del. Code	D4.5	

in terms of networking, managed services, incoming and outgoing communications and security functionalities.

After the service is deployed, the gateway is configured on the topics mentioned above. Apisix allows the user to define routes, where an endpoint is defined for receiving and forwarding client requests. Each route is also referenced to an upstream service, which is the actual service in charge of processing and answering client requests. In addition to this, when a route receives a client request, it executes other operations before sending it upwards. These operations are defined via plugins and user defined functions. Apisix offers a great number of pre-existing plugins out-of-the-box, which cover several security features that allow it to deal with many potential risks and vulnerabilities during architecture design. The following categories give an overview of the security features offered by the API gateway.

5.2.1.1 Apache APISIX security features and plugins

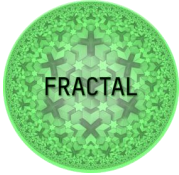
Authentication

Apisix offers several different mechanisms to prove user identity. This means that whenever a client sends a request to a particular route on the gateway, the client's identity is verified in order to check whether this user is allowed to access the requested resource. Different approaches are covered for the authentication and authorization of users, including:

- Key-auth: API Key based authentication, which is typically used to assert client identity at the service level. This method is commonly used to allow clients to consume a particular service.
- Basic-auth: User authentication method based on username and password. User data can be stored on the Apisix server in order to maintain an identity database for the environment.
- Wolf-RBAC: Is an authentication and authorization plugin based on the wolf RBAC (Role-based access control) system.
- Authz-casbin: A plugin based on Lua Casbin, which is an authorization library that supports access control models like ACL, RBAC, ABAC.
- LDAP-Auth: Authentication plugin that works with LDAP systems. This is particularly useful when managing user identity throughout a company's pre-existing infrastructure and data.

Transformation

In this category, several plugins are included to control and transform received data from the upstream services, before forwarding it to the outer world. Some of the covered mechanisms are:

	Project	FRACTAL	
	Title	FRACTAL Cybersecurity features and requirements for Fractal	
	Del. Code	D4.5	

- Response-rewrite: Rewrites the content returned by the upstream as well as Apache APISIX itself. This can be useful to update HTTP status on the response, headers, and body.
- Proxy-rewrite: Allows to rewrite exchanged content, such as the request scheme (HTTP, HTTPS), host and URI of the resources.
- gRPC-transcode: Allows to manage communications with a gRPC server. This is a Protocol Buffer based RPC communication (Remote Procedure Calls), where a client application can directly call a method on a server application on a different machine as if it was a local object, facilitating the distribution of applications and services.
- Fault-injection: Permits to elevate exceptions based on pre-defined conditions for the incoming requests, such as particular user identity, http statuses or methods.

Security

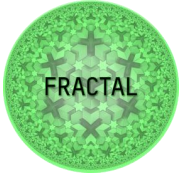
Security plugins include several mechanisms for detecting and blocking particular requests based on the origin. This origin can be identified by different properties, and some examples of these techniques are covered below:

- CORS (Cross-Origin Resource Sharing) for incoming requests. CORS is an HTTP-header based mechanism that allows a server to indicate the permitted origins for incoming requests (who or from where a user can consume a service), based on domain, scheme, or port.
- URI-blocker: Permits to define rules to block particular requests based on URI content, such as containing concrete substring or file extensions on it.
- IP blocker: Blocks incoming requests based on the origin IP and CIDRs. Rules can be established based on 'whitelist' (permit) or 'blacklist' (block) particular IPs or subnets.

Traffic

Traffic plugins include several functionalities to analyze incoming requests over time and define rules to control it. Here, some of the included mechanisms are covered:

- Limit-count: Defines rules for limiting the number of allowed requests on a given time window. With this plugin, different exceptions can be forced when incoming requests increase over different time periods.
- Limit-conn: Allows to control the maximum number of concurrent connections (requests).
- Proxy-cache: Caches upstream services requests for avoiding reprocessing every incoming request, enhancing throughput.

	Project	FRACTAL	
	Title	FRACTAL Cybersecurity features and requirements for Fractal	
	Del. Code	D4.5	

- Traffic-split: Splits incoming traffic into various upstream services.

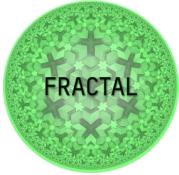
Observability

In this category, several mechanisms are included for information tracing, logging and metric gathering. The most relevant ones are described below:

- Tracers: Tracing usually refers to a particular case of logging where data movement within the application and external sources is included, thus reflecting program flow. Apisix includes integration with specialized applications, such as SkyWalking, OpenTelemetry and Zipkin.
- Loggers: Allows to push log data to defined services. Provides easy integration with multiple tools, such as HTTP-logger, TCP and UDP server loggers, MQ services loggers (such as Kafka, RocketMQ), syslog logger, and others.
- Metrics: The gateway's operation can be integrated with specialized metric tools, such as Prometheus and Datadog.

This plugin overview pretends to give a description of some of the security capabilities offered by Apisix. It is important to note that, apart from the mechanisms described above, this gateway also allows user defined functions and the creation of custom plugins, to define particular security check and logic for any use case.

Furthermore, the previous feature overview highlights the importance of including this component for the architecture design. The API gateway can provide multiple benefits in terms of security, and assist the user in the tasks of network organization and governance of its services and data.

	Project	FRACTAL	
	Title	FRACTAL Cybersecurity features and requirements for Fractal	
	Del. Code	D4.5	

6 Risk Management

Risk Management is performed according to the guidelines of ISO/IEC 27005. The result of this approach will output an OS Security Layer component, identified as WP4T44-02.

6.1 Mitigation: OS Security Layer

The OS security layer is a linux customization built via the Yocto Project¹¹, which is an open-source collaboration to build customized Linux-based systems regardless of the hardware architecture.

The OS Security Layer meets the requirements defined in deliverable 4.1., i.e., it provides the FRACTAL node with the security functions following the ISO 27005 steps.

After the compilation and implementation of the developed Yocto Security Layer, the source code of the cybersecure OS layer is generated. In addition, a cybersecurity verification script is produced. This script meets the objective of verifying that the layer has been successfully implemented and, as a result, that the OS is cybersecure.

6.2 Context establishment

The context establishment refers to the circumstances and conditions in which the risk assessment is carried out. Therefore, in this section, the FRACTAL node under consideration is examined, as well as their operation context.

6.2.1 Fractal node description

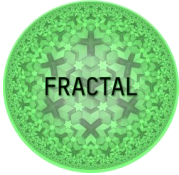
FRACTAL is a cognitive edge node for edge computing. This computing node will be the basic building block of intelligent, scalable, and non-ergodic IoT (ranging from Low-Energy Computing to High-Performance Computing Edge Nodes). This is the reason why FRACTAL node will be a scalable node following a fractal communication. Furthermore, the node is based in secure, safe, and low power features. Their main technological pillars are:

- Open-Safe-Reliable and low power node architecture.
- Low power, safety, security, and high-performance trade-off.
- Cognitive and autonomous node.
- Mutable and fractal communications.

6.2.2 Use cases

Use cases refers to the description of the potential scenarios for a component. Therefore, in this section, the use cases included in the objectives of FRACTAL will be described.

¹¹ Yocto Project, <https://www.yoctoproject.org/>

	Project	FRACTAL	
	Title	FRACTAL Cybersecurity features and requirements for Fractal	
	Del. Code	D4.5	

6.2.2.1 Use case 1: Engineering & maintenance works

Two end-to-end solutions will be developed and tested, which will allow improving the safety conditions in the construction of civil engineering works. The first solution will monitor the infrastructure with UAVs, systematizing the piloted visual inspection in near-real-time to detect building hazards. This solution will deploy a computing edge infrastructure based in microservices. The second solution will deploy sensors both in workers and machinery, placed in the construction sites, for detecting dangerous situations related to the actions carried out during the construction process, especially the workers run-over by machinery. A WSN (Wireless Sensor Network) will provide information about position and status of the workers and machinery in real-time, which will be managed through an IoT platform in order to register possible dangers and alarms and establish a protocol to follow in case of emergency.

6.2.2.2 Use case 2: AI-based controls for thermal management

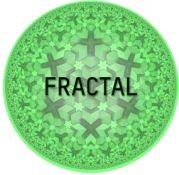
The use case deals with the development of a secure air-path control strategy exploiting data-driven models, self-learning, and self-adaption for the automotive sector. The main objective is to design intelligent control systems to reduce overall emissions and to enable the reaction to change in the environment (e.g., traffic situations, traffic light pre-emption). As such extensions to the state of the art require increased computational effort, the challenge of integrating such an intelligent system into a resource-constrained setting (e.g., electronic control units, mixed-criticality) needs to be addressed.

6.2.2.3 Use case 3: Smart meters for everyone

Smart metering is a hot topic and one of the top use cases for the internet of things. In order to support smart metering, the meters and its infrastructure around the need to be electrified which is often not the case. Electrifying the infrastructure and replacing these meters with a smart device that is connected to the internet is a big investment. In this use case, the idea is to adapt a FRACTAL node for low power operation and cost efficiency and provide a common solution for non-invasive conversion of traditional mechanical meters into IoT capable smart metering systems. The FRACTAL node will be equipped with a camera to take pictures of the traditional meter and run a pattern recognition algorithm directly on the device to identify the meter stand.

6.2.2.4 Use Case 4: Low- latency Object Detection in Industry 4.0

A widely used object detection algorithm (e.g., YOLOv3, Tiny YOLOv3) will be implemented as a FRACTAL building block that guarantees execution time with advanced HW acceleration for vision-based object detection safe systems, guaranteeing bounds of execution time are critical for functional safety systems to build a sensor fusion for edge computing use cases.

	Project	FRACTAL	
	Title	FRACTAL Cybersecurity features and requirements for Fractal	
	Del. Code	D4.5	

6.2.2.5 Use case 5: Autonomous train operation

An autonomous Urban Train use-case where artificial intelligence and high-performance computational capabilities are used to increase the dependability and the safety of the system. The objective is to apply Computer Vision (CV) and AI techniques to improve different autonomous train operation functionalities as precision stop, visual odometry, rolling stock coupling operation or person and obstacle detection- identification in railroads in order to reach a higher autonomy in urban vehicles and align them with railway European normative. CAF will use the FRACTAL approach on AI-enabled computing platforms to execute some functionalities developed in CV & AI field for autonomous train operation (driverless) which needs real-time & safety-critical computing platforms for correct performance. AI-enhanced technology will fulfil strict standards and safety regulation in order to be certified that are currently not recommended.

6.2.2.6 Use Case 6: Intelligent totem

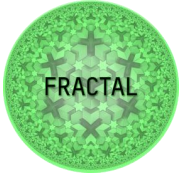
The goal of this use case is to apply the FRACTAL approach to develop an AI-based smart mobile totem, for advertisement and customer support inside shopping malls. These totems could have a disruptive impact on retail and shopping mall business providing personalized advertisements and product recommendations and driving customers towards their selected destination/product (wayfinding service). The platform will evolve into anthropomorphic robots with more advanced capabilities creating an even more immersive user experience. And it will enable their adoption not only in the retail sector but also in a smart city, providing service related to mobility, safety and security, logistics and goods delivery.

6.2.2.7 Use case 7: SPIDER autonomous robot

An AI-based path tracking algorithm will be implemented as FRACTAL building block that guarantees execution time with advanced HW acceleration, while guaranteeing bounds of execution time for safety-relevant functions. The computationally intensive relevant vehicle functions might be task dependent, like, for instance, enhanced AI based decision making techniques, sensor fusion, the creation of an occupancy grid, all of which are applicable for the demanding requirements of the automotive market. By performing the computationally intensive data processing at the edge of the network, so that the SPIDER robot only sends aggregated data to the cloud, reduces communication bandwidth requirements, and thus fosters node autonomy by reducing the cloud functionality to management and control.

6.2.2.8 Use case 8: Shuttle in Warehouse Systems

The use case employs the FRACTAL technology for a warehouse with intelligent autonomous shuttles based on cognitive computing for swarm intelligence, thereby improving availability, throughput, and safety. The goal is to improve the warehouse throughput, considering that delays in warehouse operation is critically undesirable, since it has a domino effect on the supply chain. The handling, storage, and retrieval of warehouse goods by automated shuttles are optimized using artificial intelligence

	Project	FRACTAL	
	Title	FRACTAL Cybersecurity features and requirements for Fractal	
	Del. Code	D4.5	

techniques. AI will optimally organize and analyze the masses of generated data, in order to improve the warehouse throughput.

6.2.3 Operation context

The FRACTAL node offers a mature platform to end-users for the integration and assessment of their use cases. It leverages two different platforms addressing different needs. The first platform is Xilinx VERSAL platform based on ARM, being the commercial node. It would be target for applications that need a more mature technology and SW support and need higher performance. The second platform is based on the open RISC-V PULP platform, being the customizable node. It is used for use cases with lower performance requirements. Both platforms integrate HW-level AI accelerators, and OS-level hypervisors supporting safety and security.

With this, FRACTAL node will be qualified to work under a wide variety of application domains with heterogeneous requirements, including automotive, railway or smart cities.

6.3 Risk Assessment

6.3.1 Risk Identification

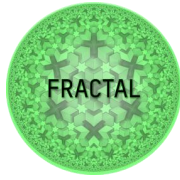
Risk identification is the process of determining the sources of security threats . Therefore, in this section, all the risk associated with the FRACTAL node in each of its use cases will be identified.

6.3.1.1 Use Cases Analysis

Table 4 provides an analysis and discussion of the cyber-security risks associated with each of the use cases (UC) proposed for the FRACTAL node.

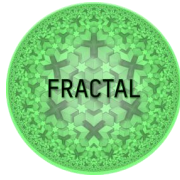
Table 4: Use cases analysis

UC	Description
UC-1: Engineering & maintenance works	<p>In this use case an end-to-end data visualization process is proposed. Two solutions are suggested, and both solutions use Fractal edge node for data collecting and transferring to a third-party system visualization or processing. Also, some data pre-processing is done on the edge node.</p> <p>The worst scenario will be a total data stream loss while data is being transmitted, this can lead to material damage or major injuries to workers, so a high availability and real time features are needed.</p> <p>Moreover, data integrity is also mandatory, so it must be protected from unwanted modifications or corruption.</p> <p>On the other hand, confidentiality is needed to prevent critical information be accessed by unwanted users.</p>



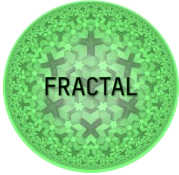
Project	FRACTAL	
Title	FRACTAL Cybersecurity features and requirements for Fractal	
Del. Code	D4.5	

UC	Description
UC-2: Air-path in combustion engines	<p>This second use case proposes a self-learning system to increase efficiency and reduce emissions of a combustion engine. The system will collect information from driving patterns and traffic infrastructure to adapt the engine parameters.</p> <p>In the worst case, a system failure will induce a degradation of the engine performance and efficiency, causing it to pollute more, so a high reliability and availability is needed.</p> <p>Because of real time computing is needed, it is important that the security countermeasures cannot affect system performance.</p> <p>As this system will work as a vehicle component, and because the data collected by the sensors are not critical, the confidentiality characteristics are not mandatory in this scenario, but data integrity is required.</p>
UC-3: Smart meters for everyone	<p>Third use case suggests the use of a Fractal edge processing node to read mechanical meters through a digital camera, so the edge node will be responsible for processing the captured image of the meter and infer the reading.</p> <p>Since image processing is the objective of the node, high-performance properties are mandatory so no performance leaks can occur when applying security countermeasures.</p> <p>The weak point in this use case will be a total data loss obtaining the readings of critical meters, for example when reading high temperature systems or flammable or explosive material storage systems. This kind of failures can cause several injuries and material damage, so a high availability and high reliability features are needed.</p> <p>Data integrity, authentication and confidentiality are also mandatory, especially when it comes to using real-time wireless connections, which must be secured as well.</p>
UC-4: Low-latency Object Detection in Industry 4.0	<p>In this fourth use case an edge node is used to pick up information from many systems, aka image sensors, CAN Bus or Ethernet, to perform a real time object detection. On the other hand, this node will enable remote monitoring so the Fractal cloud controller could get all kinds of events, alarms, or notifications through MQTT.</p> <p>Latency and throughput are critical in this case, so a high availability is totally mandatory. Authentication and confidentiality are also needed to protect unwanted users to access critical information.</p>



Project	FRACTAL	
Title	FRACTAL Cybersecurity features and requirements for Fractal	
Del. Code	D4.5	

UC	Description
	The worst case will be a total data loss which can cause that the machinery will not perform an emergency shutdown when it is needed.
UC-5: Autonomous train operation	<p>This use case proposes the automation of train stopping and safe passenger transfer with an AI powered system to approach the autonomous train operation. For that, this system will use computer vision and odometry techniques.</p> <p>Because of the hardware AI acceleration, the applied countermeasures will not greatly affect system performance.</p> <p>In the worst case, a total loss of data from the sensors can cause a train to stop where it is not supposed to, or prevent the train from stopping where needed. This can cause logistics problems, accidents, or personal injuries, so it is important to ensure the high availability of this systems.</p> <p>Moreover, data integrity is also mandatory, so it must be protected from corruption.</p>
UC-6: Intelligent totem	<p>In this use case, an AI-based smart mobile totem is proposed to enhance the experience of shopping malls and smart cities. It will provide personalized advertisements and product recommendations.</p> <p>In terms of cybersecurity this system is not a critical system so there is not necessary to have high availability features, but since personal information is collected, the data confidentiality is mandatory where, in addition, the treatment of this information must comply with the European regulation for the protection of personal data.</p>
UC-7: SPIDER autonomous robot	<p>In this use case a path tracking algorithm with accelerated hardware is proposed, for autonomous robot safe driving.</p> <p>Because of the hardware AI acceleration, the applied countermeasures will not greatly affect system performance.</p> <p>In the worst case a total loss of data from the sensors can provoke unexpected behaviour, therefore data integrity and availability are mandatory.</p>
UC-8: Shuttle in warehouse systems	<p>In this use case the cognitive FRACTAL technology is used to improve the throughput on an automated warehouse.</p> <p>Normally, warehouses must operate as quickly and efficiently as possible, so a high level of computation is expected from this system to meet the needs of high availability.</p>

	Project	FRACTAL	
	Title	FRACTAL Cybersecurity features and requirements for Fractal	
	Del. Code	D4.5	

UC	Description
	In the worst case a total loss of data from the sensors can provoke unexpected behavior, hence data integrity and availability are mandatory.

6.3.1.2 Involved assets

Once all use cases have been analyzed, a generic FRACTAL node definition will be made. This point of view will allow the security measures to be taken to be transversal to all use cases, making it unnecessary to implement different measures for each one of the situations.

For that purpose, the Figure 5 shows the identified elements that must be protected and secured in a generic FRACTAL node according with the STRIDE elements classification.

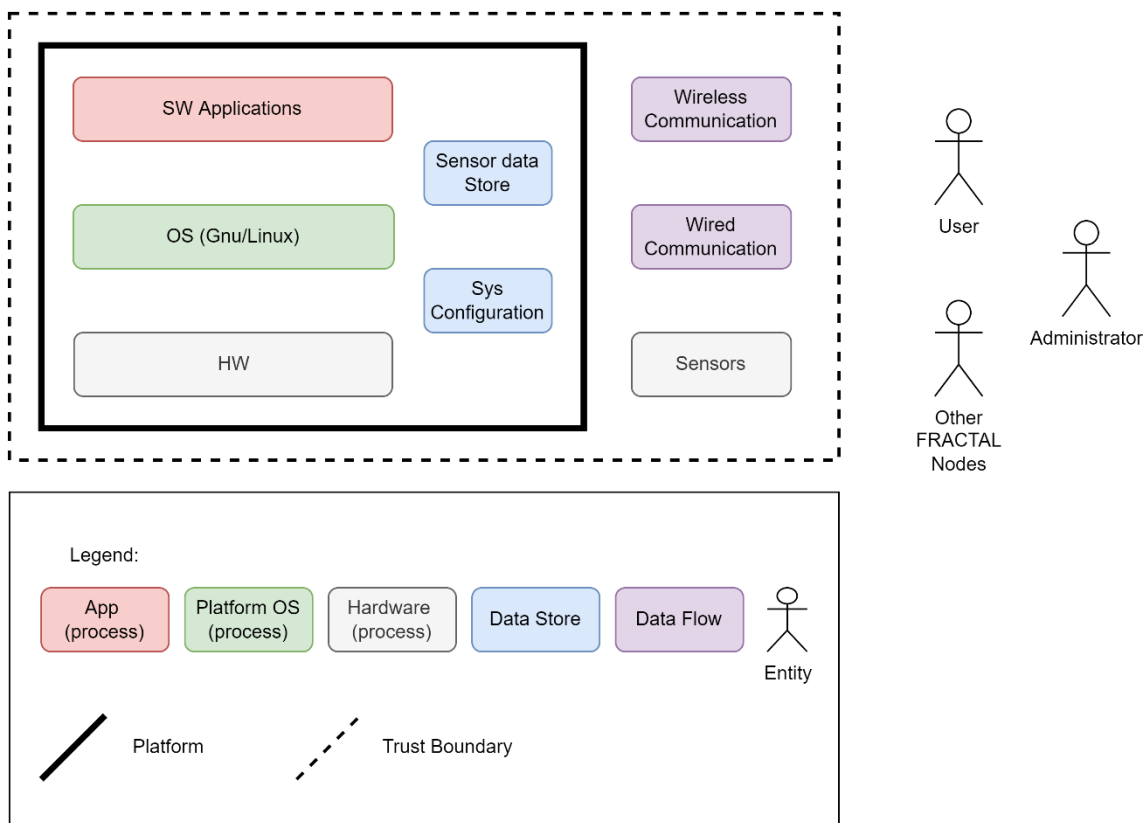
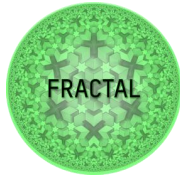


Figure 5: Asset diagram

The Table 5 lists the identified assets along with a brief description of each one.

Table 5: Asset description



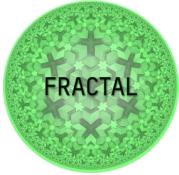
Project	FRACTAL	
Title	FRACTAL Cybersecurity features and requirements for Fractal	
Del. Code	D4.5	

Asset ID	Name	Asset Type	Description
A-1	Wireless Communication	Data Flow	All the present wireless-based communications
A-2	Wired Communication	Data Flow	All the present wired-based communications
A-3	Sensors	Process	All the sensor devices present on the use cases
A-4	Sensor Data Store	Data Store	The information stored from sensors
A-5	System configuration	Data Store	The configuration parameters which the system uses to vary its behavior.
A-6	Software Applications	Process	Application-level services and software
A-7	Operative System	Process	The operating system image (Gnu/Linux)
A-8	Hardware Platform	Process	All the hardware elements present on the FRACTAL node
A-9	User	Entity	Any person who uses the FRACTAL node
A-10	Administrator	Entity	Any person who manages the operation of the FRACTAL node
A-11	Other FRACTAL Nodes	Entity	All the rest of the FRACTAL nodes in the network

6.3.2 Risk analysis

Risk analysis is the process of examining the identified security threats in a system or organization, based on both security and safety aspects. The assessment of the risk analysis is based on the document "Security Risk analysis for Vehicular IT Systems"¹². In this section, the risks related to the identified assets of a generic FRACTAL node are analyzed. It follows the STRIDE methodology to analyze both damage and attack potential.

¹² "Security Risk Analysis for Vehicular IT Systems – A Business Model for IT Security Measures", Michael Scheibel and Marko Wolf. 7th Conference: escar – Embedded Security in Cars, November 24 - 25, 2009 – Düsseldorf

	Project	FRACTAL	
	Title	FRACTAL Cybersecurity features and requirements for Fractal	
	Del. Code	D4.5	

6.3.2.1 Damage potential

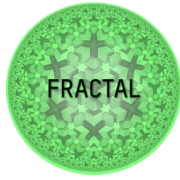
The potential damage is the estimation of the intensity of the consequences caused in the event of a successful attack. Three main factors are evaluated:

- **Personal Damage:** severity of the injuries caused to people
- **Financial Damage:** budget needed to mitigate the attack
- **Operational Damage:** severity of problems caused to the equipment

The potential damage of all assets involved in the generic FRACTAL node is analyzed and estimated in the Table 6.

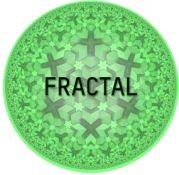
Table 6: Damage Potential

Asset ID	Asset Name	Asset Type	STRIDE	Impact Description	Damage Potential
A-1	Wireless communication	Data flow	S	-	#N/D
			T	This attack could improve spoofing attacks. May require maintenance of the unit.	Critical
			R	-	#N/D
			I	Disclosure of information captured on wireless communications system may reveal sensitive information that if not properly protected would allow an attacker to perform unwanted actions.	Insignificant
			D	Disruption of wireless networks may cause the system to stop operating, receiving updates, or transmitting critical information. The affected infrastructure may have to be maintained.	Critical
			E	-	#N/D
A-2	Wired communication	Data flow	S	-	#N/D
			T	Tampering with wired communications can be detrimental to the whole system, including microservices and the operating system, as they may stop working or have unexpected behavior. This can cause material and personal damage, even requiring replacement of the unit and part of the system.	Critical
			R	-	#N/D
			I	Disclosure of information captured on communications buses may reveal sensitive information that if not properly protected would allow an attacker to perform unwanted actions.	Insignificant
			D	The failure of wired networks can lead to personal injury, operational damage and compromise safety and security. Maintenance work on the installation will therefore be required.	Critical
			E	-	#N/D
A-3	Sensors	Hardware	S	Makes a fraudulent measurement look like a legitimate one. This could affect the comfort of operation by altering the data being recorded. Maintenance is required.	Critical
			T	It may cause the sensor to stop working causing a problem in the operation of the whole system. It could cause several operational damages and affect the safety and security of the system. Requires maintenance.	Critical
			R	Loss of the authenticity of the sensor. This could cause a damage in the operation of the whole system and affect its safety and security. Requires maintenance.	Critical
			I	It facilitates the extraction of machine secrets or the deletion of the entire database tables. The consequences are very damaging to a company.	Insignificant
			D	It leaves no space available for the normal operating process of the sensor. The denial of service, in whole or in part, in a sensor may refer to damage to public health and safety.	Critical
			E	That elevation of privileges gives root functions to the attacker, which can influence the normal operation of the sensor. This could affect the integrity of the people or of the equipment.	Medium
A-4	Sensor data store	Data Store	S	Makes a fraudulent measurement look like a legitimate one. This could affect the comfort of operation by altering the data being recorded. Maintenance is required.	Critical
			T	This could provoke an anomalous behavior of the complete system. It could cause some injuries or affect the comfort of operation.	Critical
			R	The data stored on the database can be considered invalid or misleading. It may cause several problems that should require maintenance.	Medium
			I	It facilitates the extraction of machine secrets or the deletion of the entire database tables. The consequences are very damaging to a company.	Medium



Project	FRACTAL	
Title	FRACTAL Cybersecurity features and requirements for Fractal	
Del. Code	D4.5	

Asset ID	Asset Name	Asset Type	STRIDE	Impact Description	Damage Potential
			D	Interrupt the store's normal operation, affecting the monitoring of the whole system. Maintenance is required.	Medium
			E	-	#N/D
A-5	System configuration	Data Store	S	Replacement of the system configuration will provoke anomalous behavior. It may require maintenance of the unit. Its application may cause personal injury and operational damage.	Critical
			T	Replacement of the system configuration will provoke anomalous behavior. It may require maintenance of the unit. Its application may cause personal injury and operational damage.	Critical
			R	It may have important legal consequences.	Medium
			I	This information may support future initial access to an object or system. Can cause serious operational damage in the post-access stages.	Medium
			D	It may cause the system to stop working properly. It can affect the comfort of the system.	Medium
			E	-	#N/D
A-6	Software Applications	Process	S	The installation of unauthorized or third-party software can lead to safety and security breaches. This can cause instability in the system and may require revision and maintenance.	Critical
			T	A malicious application could have access to and control over the entire system. This can cause instability in the system and may require revision and maintenance.	Critical
			R	The data stored on log files can be considered invalid or misleading. This can affect the comfort of operation and requires maintenance.	Medium
			I	This may result in the leakage of user data. It could cause light injuries, but it does not have effect in the normal operation of the system.	Medium
			D	Exhausts the system's resources. This may alter the operational comfort of the system and cause large expenses.	Critical
			E	Gets access to more resources or functionality than allowed. It could cause large expenses and needs maintenance.	Critical
A-7	Operative System	Process	S	It causes instability and undesired behavior in the system. Also, it may result in damage to property and personal injury, rendering the system unusable and requiring subsequent maintenance.	Critical
			T	It causes abnormal behavior of the whole system, resulting in serious accidents with personal injury and damage to property.	Critical
			R	In addition to the possible accident or injury caused, it could have legal implications.	Critical
			I	An information leak could lead to a security problem in many of the installed devices, requiring an upgrade or even replacement of this equipment.	Critical
			D	Leaves communication without service, impeding necessary data from being transmitted. Although it would not cause damage to the system, it could require maintenance or even replacement of the unit.	Critical
			E	Provides full system access and control, which could lead to serious accidents involving persons.	Critical
A-8	Hardware Platform	Hardware	S	Since untested hardware can cause instability problems, both safety and security can be compromised, rendering the equipment unusable and requiring replacement.	Critical
			T	Tampering with the hardware can lead the system into unintended states and compromise both safety and security, rendering the equipment totally unusable and requiring replacement or repair.	Critical
			R	It may have important legal implications.	Critical
			I	If a unit is successfully reverse engineered, clones of the unit could be generated. Unauthorised copying may cause financial losses.	Critical
			D	The denial of service in a hardware platform may refer to damage to public health and safety. The unit must be replaced or repaired.	Critical
			E	It makes necessary to replace the unit	Critical
A-9	User	Entity	S	May result in the theft of user or node information	Medium
			T	-	#N/D
			R	It may result in an initial access to the system that has an impact on the operation of the whole system.	Critical
			I	-	#N/D
			D	-	#N/D
			E	-	#N/D
A-10	Administrator	Entity	S	A malicious user could gain unauthorized network access, preventing legit users from accessing/using the device.	Critical
			T	-	#N/D
			R	Insertion of malicious code with impact on the operation of the whole system.	Critical
			I	-	#N/D
			D	-	#N/D
			E	-	#N/D

	Project	FRACTAL	
	Title	FRACTAL Cybersecurity features and requirements for Fractal	
	Del. Code	D4.5	

Asset ID	Asset Name	Asset Type	STRIDE	Impact Description	Damage Potential
			€	-	#N/D
A-11	Other FRAC-TAL Nodes	Entity	S	Makes a fraudulent node look like a legitimate one. It requires maintenance.	Critical
			ƒ	-	#N/D
			R	Erroneous data flowing over the network, affecting the comfort of use.	Critical
			£	-	#N/D
			Ɔ	-	#N/D
			E	-	#N/D

6.3.2.2 Attack potential

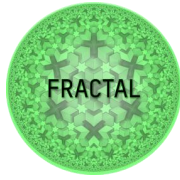
The attack potential determines the effort an attacker must expend to exploit a given attack path. Among the metrics to be evaluated are the following factors:

- **Elapsed Time:** time required to perform an attack.
- **Expertise:** level of experience required to perform an attack.
- **Information about target:** the available information about the attack.
- **Access to target:** the accessibility of the objective.
- **Equipment:** the required equipment to perform an attack.

The attack potential of all assets involved in the generic FRACTAL node is analyzed and estimated in the Table 7.

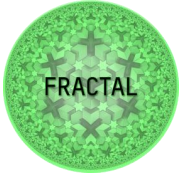
Table 7: Attack Potential

Asset ID	Asset Name	Asset Type	STRIDE	Impact Description	Attack Potential
A-1	Wireless communication	Data flow	S	-	#N/D
			T	Modifies data flowing over the network through wireless transmission system. (Wi-fi, Zigbee, Bluetooth...)	High
			R	-	#N/D
			I	Physical attack consisting of extracting, capturing, and disseminating the information transmitted through the wireless network. Requires being in close proximity from the wireless communications system installation. A person with a proficient level of knowledge and several weeks is considered.	Enhanced-Basic
			D	Consume network resources through wireless communication, affecting the normal operation of the network. An expert with special equipment will be required.	Moderate
			E	-	#N/D
A-2	Wired communication	Data flow	S	-	#N/D
			T	Physical attack on proprietary protocols. Requires access to the wired communications system installation. A person with an advanced level of knowledge and several days is considered.	High
			R	-	#N/D
			I	Physical attack consisting of extracting, capturing, and disseminating the information transmitted through the communications buses. Requires access to the wired communications system from the facility's maintenance room. A person with a proficient level of knowledge and several days is considered.	High
			D	Physical attack, accessing the device and damaging or disconnecting wired communication systems. It is considered that a person without special knowledge and without special equipment will be able to carry out the attack.	Moderate
			E	-	#N/D
A-3	Sensors	Hardware	S	Change the measurements taken by sensors from an external source. A person without special knowledge with access to the measured entity will be able to perform the attack in several weeks.	Beyond High-Rare
			T	Tampering with the power supply level (by software or physically). A person with special knowledge and with access to the facilities where the sensor is located will be able to perform the attack in several weeks.	Moderate



Project	FRACTAL	
Title	FRACTAL Cybersecurity features and requirements for Fractal	
Del. Code	D4.5	

Asset ID	Asset Name	Asset Type	STRIDE	Impact Description	Attack Potential
			R	Physical attack consisting of changing the location of the sensor or making changes to it without subsequent registration. A person with advanced knowledge and several months of work is considered.	Beyond High-Rare
			I	Exploit bugs to read and publish information. A person with advanced knowledge and several weeks of work is considered.	Moderate
			D	Inserting a process in the sensor that absorbs its memory (RAM or disk) or CPU. It is considered a person with advanced knowledge and some specialized equipment.	Beyond High-Rare
			E	Use valid credentials to access root functions. The valid credentials of some sensors are information available in public repositories as they have not been changed from their factory default value. That means that a person with proficient experience should be able to make an elevation of privileges if he gets initial access.	High
A-4	Sensor data store	Data Store	S	Access to the device and modification of real sensor data by fraudulent information. A person with advanced knowledge and several weeks of work is considered.	Moderate
			T	Modification of the data generated by the sensor and stored. A person with advanced knowledge and several weeks of work is considered.	Moderate
			R	Storing sensor data in the data store without registration. A person with advanced knowledge and several months of work is considered.	High
			I	Take advantage of bad file access permissions and get data from logs/temp files or swap files. It is considered an expert with advanced knowledge some months of work.	High
			D	Misappropriation of data storage space from an external source. It is considered an expert profile with several weeks of work and access to public information.	Moderate
			E	-	#N/D
A-5	System configuration	Data Store	S	Accessing the device and inserting a configuration file into the system to cause the system to rely on these fake configuration parameters. Considered a specialist with access to restricted information with a dedication of several weeks.	High
			T	Access to the device either during its initial configuration or during operation to manipulate configuration parameters. Considered an advanced specialist with access to sensitive information with a dedication of several weeks.	High
			R	Reconfiguration of the system by manipulating the configuration parameters without registration. Considered an expert with access to restricted information and with a dedication of few months.	High
			I	Take advantage of missing or inappropriate access-control list (ACLs) and publish it. It is considered an expert profile with access to sensitive information and a dedication of a few weeks.	High
			D	Makes enough configuration requests to slow the system or deny its service. It is considered a proficient with several weeks of dedication and access to restricted information.	Moderate
			E	-	#N/D
A-6	Software Applications	Process	S	Access to the device and installation of unauthorized software. It is considered a profile of an expert with weeks of work to successfully install third-party software.	Moderate
			T	Access to the device and manipulation of the installed software in the system. Requires an expert person with access to sensitive information and some weeks of work.	High
			R	Manipulate general data without track or log properly. It is considered a profile of an expert with weeks of work.	High
			I	Theft of information by exploiting software bugs or reading error messages. It is considered an expert person with access to sensitive information and weeks of work.	High
			D	Flood the application with superfluous requests. It is considered an expert person with access to sensitive information and some months of work.	High
			E	Exploit vulnerabilities to gain higher privilege accounts, edit scripts that are launched with high privileges or misuse configuration errors. Requires an expert to perform the attack and months of work.	High
A-7	Operating System	Process	S	Access to the device and install a different operating system. This requires the work of multiple experts and some months of work.	High
			T	Access the device and manipulate the operating system. It requires an expert working some weeks and specialized equipment.	High
			R	Make changes to the operating system without registration. Requires a person with advanced knowledge to perform the attack.	Beyond High-Rare
			I	Theft of information by exploiting bugs or reading error messages. An expert requiring access to sensitive information with a few weeks of work is considered.	High
			D	Exploit vulnerabilities against business logic. It is considered an expert with access to available public information and to have worked for several months.	High
			E	Access to the device and create or modify system processes to maintain network persistence. It is considered a person with advanced knowledge, access to restricted information and several months of work.	High

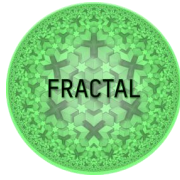
	Project	FRACTAL	
	Title	FRACTAL Cybersecurity features and requirements for Fractal	
	Del. Code	D4.5	

Asset ID	Asset Name	Asset Type	STRIDE	Impact Description	Attack Potential
A-8	Hardware Platform	Hardware	S	Physical attack, theft of a unit and replacement of hardware. A profile of an expert person with weeks of dedication, highly specialized equipment, with access to restricted information is considered.	High
			T	Physical attack consisting of access and manipulate internal hardware. It is considered a profile of an expert person with weeks of dedication, highly specialized equipment and access to restricted information.	High
			R	Physical manipulation over the hardware without authorization. It is considered a person with advanced knowledge with bespoke equipment.	Beyond High-Rare
			I	Physical attack, consisting of theft of a unit, disassembling and studying it. To extract information from a unit, it is considered necessary to have several months of expertise and dedication to reverse engineer the unit.	Beyond High-Rare
			D	Physical attack, accessing a unit and disconnecting or damaging it. By accessing the maintenance room, it could be very easy to damage or destroy a unit. No special knowledge is required, and the attack can be carried out in a matter of days without specialized equipment.	Moderate
			E	Physical attack. Theft of a unit, disassembly, and access to unprotected or debug interfaces. Advanced knowledge and specialized equipment are required to carry out the attack.	High
A-9	User	Entity	S	Taking over an account by impersonating a user. It requires an expert person with standard equipment and weeks of work.	Enhanced-Basic
			⌘	-	#N/D
			R	Makes malicious actions and claims to be a fraud victim. It does not require advanced knowledge.	Moderate
			⌚	-	#N/D
			⌘	-	#N/D
A-10	Administrator	Entity	S	A user declares itself as administrator. It requires expert knowledge.	Moderate
			⌘	-	#N/D
			R	Claims to be a fraud victim.	Moderate
			⌚	-	#N/D
			⌘	-	#N/D
A-11	Other FRAC-TAL Nodes	Entity	S	Impersonate a node with ARP spoofing, IP spoofing or DNS spoofing mechanisms. It requires a person with some knowledge and restrictive information.	Moderate
			⌘	-	#N/D
			R	Blaming a node for something that it has done itself. It requires an expert with restricted information and some weeks of work.	High
			⌚	-	#N/D
			⌘	-	#N/D

6.3.3 Risk evaluation

The risk evaluation is the process in which the risks associated to each asset are computed qualitatively. Risks are usually estimated on an established scale that estimates probability (for instance: low, medium, high), and risks are also usually categorized based on the source of it or on the effect to the company. Whereas qualitative risk assessments utilize knowledge and experience to determine risk probability, a quantitative risk assessment relies on objective, measurable data to provide insights into your risk management process. In terms of cybersecurity attack probability cannot be computed since the since the actions carried out by cyber-attackers and their possible motivations (e.g. political, economical) cannot be known beforehand.

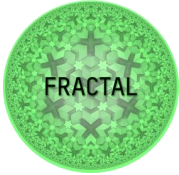
this information, a risk level evaluation associated with the exploitation of each attack path identified is obtained, as shown in the Table 8.



Project	FRACTAL	
Title	FRACTAL Cybersecurity features and requirements for Fractal	
Del. Code	D4.5	

Table 8: Risk Evaluation

Asset ID	Asset Name	Asset Type	STRIDE	Impact Description	Attack Potential	Damage Potential
A-1	Wireless communication	Data flow	S	#N/D	#N/D	#N/D
			T	High	Critical	Undesirable
			R	#N/D	#N/D	#N/D
			I	Enhanced-Basic	Insignificant	Tolerable
			D	Moderate	Critical	Undesirable
			E	#N/D	#N/D	#N/D
A-2	Wired communication	Data flow	S	#N/D	#N/D	#N/D
			T	High	Critical	Undesirable
			R	#N/D	#N/D	#N/D
			I	High	Insignificant	Negligible
			D	Moderate	Critical	Undesirable
			E	#N/D	#N/D	#N/D
A-3	Sensors	Hardware	S	Beyond High-Rare	Critical	Tolerable
			T	Moderate	Critical	Undesirable
			R	Beyond High-Rare	Critical	Tolerable
			I	Moderate	Insignificant	Tolerable
			D	Beyond High-Rare	Critical	Tolerable
			E	High	Medium	Tolerable
A-4	Sensor data store	Data Store	S	Moderate	Critical	Undesirable
			T	Moderate	Critical	Undesirable
			R	High	Medium	Tolerable
			I	High	Medium	Tolerable
			D	Moderate	Medium	Undesirable
			E	#N/D	#N/D	#N/D
A-5	System configuration	Data Store	S	High	Critical	Undesirable
			T	High	Critical	Undesirable
			R	High	Medium	Tolerable
			I	High	Medium	Tolerable
			D	Moderate	Medium	Undesirable
			E	#N/D	#N/D	#N/D
A-6	Software Applications	Process	S	Moderate	Critical	Undesirable
			T	High	Critical	Undesirable
			R	High	Medium	Tolerable
			I	High	Medium	Tolerable
			D	High	Critical	Undesirable
			E	High	Critical	Undesirable
A-7	Operative System	Process	S	High	Critical	Undesirable
			T	High	Critical	Undesirable
			R	Beyond High-Rare	Critical	Tolerable
			I	High	Critical	Undesirable
			D	High	Critical	Undesirable
			E	High	Critical	Undesirable
A-8	Hardware Platform	Hardware	S	High	Critical	Undesirable
			T	High	Critical	Undesirable
			R	Beyond High-Rare	Critical	Tolerable
			I	Beyond High-Rare	Critical	Tolerable
			D	Moderate	Critical	Undesirable
			E	High	Critical	Undesirable
A-9	User	Entity	S	Enhanced-Basic	Medium	Undesirable

	Project	FRACTAL	
	Title	FRACTAL Cybersecurity features and requirements for Fractal	
	Del. Code	D4.5	

Asset ID	Asset Name	Asset Type	STRIDE	Impact Description	Attack Potential	Damage Potential
			T	#N/D	#N/D	#N/D
			R	Moderate	Critical	Undesirable
			I	#N/D	#N/D	#N/D
			D	#N/D	#N/D	#N/D
			E	#N/D	#N/D	#N/D
A-10	Administrator	Entity	S	Moderate	Critical	Undesirable
			T	#N/D	#N/D	#N/D
			R	Moderate	Critical	Undesirable
			I	#N/D	#N/D	#N/D
			D	#N/D	#N/D	#N/D
A-11	Other FRACTAL Nodes	Entity	S	Moderate	Critical	Undesirable
			T	#N/D	#N/D	#N/D
			R	High	Critical	Undesirable
			I	#N/D	#N/D	#N/D
			D	#N/D	#N/D	#N/D
			E	#N/D	#N/D	#N/D

6.4 Risk Treatment

Risk treatment is the process in which a strategic decision must be taken on the identified risks. Therefore, this section will identify the security countermeasures (CM) for the vulnerable assets of the FRACTAL node. Then, the implementation process of those countermeasures is described.

6.4.1 Security Countermeasures

In order to carry out the risk treatment, a set of countermeasures have been defined, as shown in Table 9. These countermeasures are implemented in a security layer via the Yocto Project.

Only assets classified with an undesirable or intolerable risk value in the risk evaluation will have a mitigation requirement. Tolerable or negligible risks will have no treatment so no countermeasure will be defined.

The countermeasures to be implemented are divided into three modules: (1) secure communications, (2) authentication and authorization, and (3) firewall. An audit system will not be implemented at the fractal node level because it would limit the view of events throughout the system. The audit system is expected to be logged at network level. This solution allows to observe what is happening in the whole system, while respecting the scalability of the fractal nodes.

Table 9 summarizes the specific countermeasures to be applied in each module.

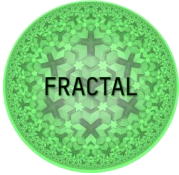
	Project	FRACTAL	
	Title	FRACTAL Cybersecurity features and requirements for Fractal	
	Del. Code	D4.5	

Table 9: Countermeasure description

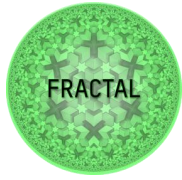
CM ID	CM Name	CM Description
C-1	Secure communications	OpenSSH is based on the Secure Shell (SSH) protocol, which provides a secure channel over an unsecured network in a client-server architecture. This CM involves install and configure OpenSSH toolkit for secure FRACTAL communication.
C-2	Authentication & Authorization	Best practices dictate to use as many user accounts as users need to access to the machine. At the same time, if several users need to share access to certain system resources, it is also necessary to manage the corresponding group accounts. In addition, the following CM must be configured for all users, including other FRACTAL nodes: <ul style="list-style-type: none"> • Elliptic curve-based authentication as an energy-efficient authentication scheme • Role-based Access Control (RBAC) authorization model
C-3	Firewall	A firewall is a network security system that monitors and controls all inbound and outbound network traffic based on predetermined security rules. This CM involves install and configure the <i>nftables</i> firewall.

Those countermeasures implement a set of technical measures to avoid risks and bad configurations of FRACTAL Node components, such as spoofing, tampering, denial of service and elevation of privileges.

Table 10 summarizes the list of assets on which apply the countermeasures and the threats they counter.

Table 10: Countermeasures and related assets

CM ID	CM Name	Related Assets	Addressed Threat
C-4	Secure communications	A-1	Tampering
		A-2	Tampering
		A-11	Spoofing
Repudiation			
C-5	Authentication & Authorization	A-3*	Tampering
		A-4	Spoofing
			Tampering
		A-5	Spoofing
Tampering			



Project	FRACTAL	
Title	FRACTAL Cybersecurity features and requirements for Fractal	
Del. Code	D4.5	

CM ID	CM Name	Related Assets	Addressed Threat
		A-6	Spoofing
			Tampering
			Elevation of Privileges
		A-7	Spoofing
			Tampering
			Information Disclosure
			Elevation of Privileges
		A-8**	Spoofing
			Tampering
			Elevation of Privileges
		A-9	Spoofing
			Repudiation
A-10	Spoofing		
	Repudiation		
A-11	Spoofing		
	Repudiation		
C-6	Firewall	A-1	Denial of Service
		A-2	Denial of Service
		A-4	Denial of Service
		A-5	Denial of Service
		A-6	Denial of Service
		A-7	Denial of Service

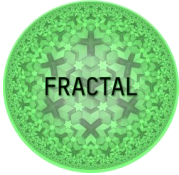
* Sensors (asset A-3) are not under the control of the FRACTAL node. This means that countermeasures cannot be applied internally. It is recommended to apply externally the countermeasure C-2 to them to protect them from attacks such as tampering.

** On the hardware platform (asset A-8) a denial of service can be executed physically. This type of attack could not be countered by technical measures. It is necessary to apply environmental measures and physical security in addition to the technical ones.

6.4.2 Transversal Yocto Security Layer Implementation

Yocto Project architecture is based on layers. Each layer contains both configuration data (*.conf) and recipes metadata (*.bb). Configuration data defines the settings that determine the OpenEmbedded build process. Recipes files hold details about specific pieces of software.

Yocto implements Poky as a reference distribution. Poky content could be modified, added, or removed to suit the needs of each application. To implement a Poky

	Project	FRACTAL	
	Title	FRACTAL Cybersecurity features and requirements for Fractal	
	Del. Code	D4.5	

distribution, it must be cloned from the Poky git repository¹³. Concretely, *dunfell* version has considered since it is the last stable release.

For application to FRACTAL, it is also necessary to clone the dependencies *meta-openembedded*¹⁴ and *meta-security*¹⁵. Those dependencies also need the *dunfell* version to be compliant.

Finally, the OS Security Layer, called *meta-fractal*, is added to the Poky distribution. It is appended during the operating system building process. The OS Security Layer is platform independent, so it can be used in most applications where Yocto is used to compose the FRACTAL Node operating system.

The *meta-fractal* layer directories are structured as follows:

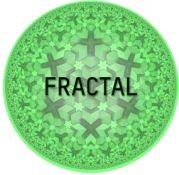
- ***meta-fractal/conf***. It is a configuration directory which defines the specific layer and distro configurations over the FRACTAL project.
- ***meta-fractal/recipes-connectivity***. This recipe implements security tasks from the package *openssh* for both secure communications and authentication and Authorization countermeasures.
- ***meta-fractal/recipes-core***
 - ***base-files***. This recipe configures the basic filesystem hierarchy. Specifically, it implements security tasks related to the authentication and authorization countermeasure.
 - ***busybox***. This recipe provides the *net-tools* package for administration.
 - ***images***. This recipe covers the packages installation. It appends the *useradd*, *group-core-ssh-openssh*, *package-management*, *nftables*, *sudo* and *btfs-tools* packages to the operative system.
 - ***useradd***. This recipe configures users, groups, and home directories.
- ***meta-fractal/recipes-extended***. This recipe adds the users to the sudoers file.
- ***meta-fractal/recipes-filter***. This recipe configures countermeasures related with the Firewall. It includes the default firewall configuration file, as well as the *sysvinit* service file to load the configuration file at the start.
- ***meta-fractal/recipes-kernel***. This recipe adds arm-autonomy kernel support, for the Firewall countermeasure.

Yocto Project works together with OpenEmbedded. OpenEmbedded is a build system to achieve image and SDK generation. It has two components associated with it. First, it uses BitBake component to build images by parsing and executing the recipes metadata and configuration files. Complementing it, the build system has the OpenEmbeddedCore (OE-core) component. OE-core is a common layer of metadata that operates as a carefully controlled and quality-assured core set of recipes.

¹³ <https://git.yoctoproject.org/poky>

¹⁴ <https://github.com/openembedded/meta-openembedded>

¹⁵ <https://git.yoctoproject.org/meta-security/>

	Project	FRACTAL	
	Title	FRACTAL Cybersecurity features and requirements for Fractal	
	Del. Code	D4.5	

To create the final Linux distribution, there is a detailed process to build the image. First, the initialization of the build environment must be executed. From within the *poky* directory, it must be running the *oe-init-build-env* script. This script creates the default configuration files in the build directory if they are not created. This configuration files are:

- ***conf/local.conf***. This file includes common configuration options, such as the machine selection to target the build with, the directory to place downloads, the policy configuration for the distribution, the package management configuration, or the disk space monitoring during the build, among others. This file needs some changes applied to FRACTAL system:

```
Build Configuration:
BB_VERSION           = "1.46.0"
BUILD_SYS            = "x86_64-linux"
NATIVELSBSTRING     = "ubuntu-20.04"
TARGET_SYS          = "x86_64-fractal-linux"
MACHINE              = "qemux86-64"
DISTRO               = "fractal"
DISTRO_VERSION       = "1.0.0"
TUNE_FEATURES        = "m64 core2"
TARGET_FPU           = ""
```

- ***conf/bblayers.conf***. This file includes the definition of the metadata layers to build the final distribution. For the FRACTAL System, the layers *meta-openembedded/meta-oe*, *meta-openembedded/meta-networking*, *meta-openembedded/meta-python*, *meta-security/meta-security-compliance* and *meta-fractal* are appended to the default ones. The final layer structure is:

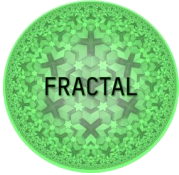
```
meta
meta-poky
meta-yocto-bsp
meta-oe
meta-networking
meta-python
meta-security-compliance
meta-fractal
```

Once the configuration is complete, the *bitbake* command is executed by selecting the *fractalimage* target to start the build. The result is a FRACTAL system-specific, platform-independent image and SDK.

6.4.3 Transversal Yocto Security Layer Verification

The verification process is based on approve or deny the validity of each implemented countermeasure in the FRACTAL OS. For verifying the operation of the Yocto Security Layer, a set of tests is implemented via bash shell scripts.

The architecture of the verification tests is divided into three sections, one for each countermeasure: (1) secure communications verification (*Test/SecComms*), (2)

	Project	FRACTAL	
	Title	FRACTAL Cybersecurity features and requirements for Fractal	
	Del. Code	D4.5	

authentication and authorization (*Test/Auth*), and (3) firewall (*Test/Firewall*). Each directory contains a set of bash shell scripts with technical verification measures to check if each specific countermeasure has been implemented successfully.

The whole verification process is controlled by a monitoring and control script, called *RunTests.sh*. This script is responsible for executing all independent verification tests and returning the result obtained for each one. If the checked countermeasure has been successfully implemented through the Yocto Security Layer, a PASS result will be returned. Otherwise, a FAIL result shall be returned.

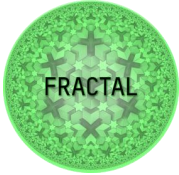
Figure 6 shows the results obtained during the Yocto Security Layer verification. Out of a total of 25 tests executed, there are 25 successful tests, and none failed.

```

sysadmin@qemux86-64:~/fractal-verification$ sudo bash ./Run_Tests.sh
Running SecComms tests
SecComms_01.sh - Ensure OpenSSH is installed.....PASS
SecComms_02.sh - Ensure permissions in /etc/ssh/sshd_config are 0600.....PASS
SecComms_03.sh - Ensure protocol version is 2.....PASS
SecComms_04.sh - Ensure SSH MaxAuthTries is 4 or less.....PASS
SecComms_05.sh - Ensure SSH root login is disabled.....PASS
SecComms_06.sh - Ensure Empty Passwords are not allowed.....PASS
SecComms_07.sh - Ensure users are not allowed to Set Environment Options.....PASS
SecComms_08.sh - Ensure only approved cipher in counter mode are used.....PASS
Running Auth tests
Auth_01.sh - Ensure that only strong MAC algorithms are used.....PASS
Auth_02.sh - Ensure only strong Key Exchange algorithms (Elliptic Curve) are used.....PASS
Auth_03.sh - Ensure sudo is installed.....PASS
Auth_04.sh - Ensure user groups and default user accounts exist.....PASS
Auth_05.sh - Ensure sysadmin is added to sudoers file.....PASS
Auth_06.sh - Ensure default user umask is 027 or more restrictive.....PASS
Auth_07.sh - Ensure default user shell timeout is 900 seconds or less.....PASS
Auth_08.sh - Ensure /sbin and /usr/sbin are added to $PATH for the root user.....PASS
Running Firewall tests
Firewall_01.sh - Ensure nftables is installed.....PASS
Firewall_02.sh - Ensure nftables is enabled.....PASS
Firewall_03.sh - Ensure iptables rules are flushed.....PASS
Firewall_04.sh - Ensure a table exists.....PASS
Firewall_05.sh - Ensure all base chains exists [hook input/forward/output].....PASS
Firewall_06.sh - Ensure loopback traffic is configured.....PASS
Firewall_07.sh - Ensure outbound and established connections are configured.....PASS
Firewall_08.sh - Ensure default deny firewall policy.....PASS
Firewall_09.sh - Ensure nftables default configuration file exists.....PASS
Total tests executed: 25
Successful tests: 25
Failed tests: 0

```

Figure 6: Verification results of the Yocto OS

	Project	FRACTAL	
	Title	FRACTAL Cybersecurity features and requirements for Fractal	
	Del. Code	D4.5	

7 GDPR Compliance

This section presents a Use Case wide analysis on the compliance to General Data Protection Regulation (GDPR). The GDPR is the European regulation that governs the way in which companies and other organizations process personal data. In case there is any risk for the rights and freedoms of natural persons, a Data Protection Impact Assessment (DPIA) consisting of an assessment of the level of risk and the determination of appropriate measures to mitigate it, will be conducted.

7.1 Regulatory framework

- REGULATION 2016/679/EU
- WP248 - Guidelines on data protection impact assessment and determination of the possibility that the processing "may present a high risk" for the purposes of Regulation (EU) 2016/679

7.2 Definitions

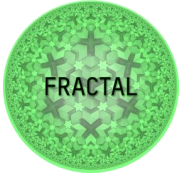
The article 3 of regulation provides a lot of definitions in the GDPR context. They will be not mentioned here, but it is useful to report the most important:

- Personal Data (including particular categories and data relating to criminal convictions and offenses);
- DPIA (Data Protection Impact Assessment).

The Table 11 reports definition of personal data.

Table 11: List of Personal Data

PERSONAL DATA
Data that allow direct identification - such as personal data (name and surname, images, etc. - and data that allow indirect identification, such as an identification number (for example, the tax code, the IP address, the identification number).
Data falling into particular categories: this is the so-called data "sensitive", i.e., those that reveal racial or ethnic origin, religious or philosophical beliefs, political opinions, trade union membership, relating to health or sexual life. Regulation (EU) 2016/679 (article 9) also included in the notion genetic data, biometric data and those relating to sexual orientation.
Data relating to criminal convictions and offenses: these are the so-called data "judicial", i.e., those that can reveal the existence of certain judicial measures subject to registration in the criminal record (for example, definitive criminal convictions, conditional release, prohibition or obligation to stay, alternative measures to detention) of the quality of accused or suspected person. Regulation (EU) 2016/679 (article 10) includes in this concept the data relating to criminal convictions and offenses or related security measures.

	Project	FRACTAL	
	Title	FRACTAL Cybersecurity features and requirements for Fractal	
	Del. Code	D4.5	

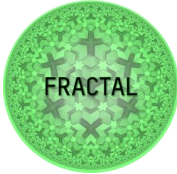
The DPIA is an assessment aiming at describing the processing of personal data, assessing its necessity and proportionality, as well as managing any risk for the rights and freedoms of natural persons deriving from it, by carrying out an analysis of the risk level and determining the appropriate measures to mitigate it. This is a preliminary assessment carried out by the Data Controller in relation to the impacts of a processing violating the protection measures. The DPIA must be viewed as a fundamental tool in order to implement the approach to the protection of personal data recalled by the European regulation and strongly based on the principle of accountability.

7.3 Workflow

Figure 7 summarizes the workflow of the analysis conducted for each Use Case. A questionnaire was provided to each Use Case in order to conduct a preliminary assessment, define the data treatment and understand if a Data Protection Impact Assessment was needed.

The major phases of this workflow are:

- Conduct a preliminary risk assessment;
- Define if a DPIA is needed;
- Conduct a DPIA (if needed).

	Project	FRACTAL
	Title	FRACTAL Cybersecurity features and requirements for Fractal
	Del. Code	D4.5

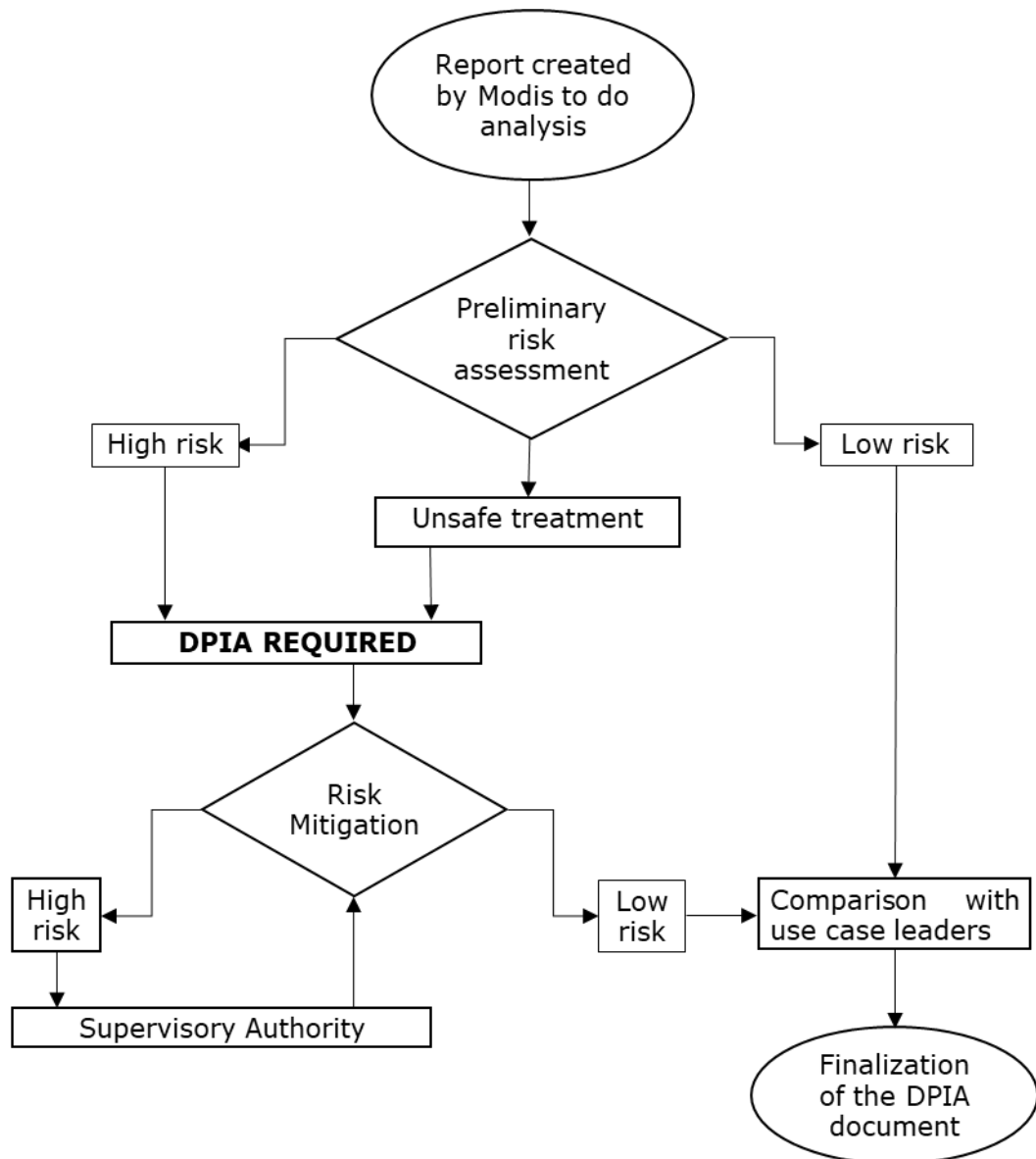


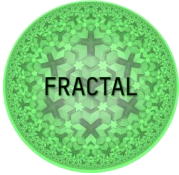
Figure 7: Activity workflow

7.3.1 Preliminary risk assessment

The preliminary risk assessment consists in two steps.

Step 1 aims to describe and analyze the data treatment defining:

- Stakeholders;
- Purpose of the treatment;
- Description of the treatment and information flows;
- Data object of the treatment;

	Project	FRACTAL	
	Title	FRACTAL Cybersecurity features and requirements for Fractal	
	Del. Code	D4.5	

- Method of treatment;
- Operations performed;
- Data processed storage;
- Business processes involved in the treatment.

Step 2 called “conformity assessment” aims to analyze the data management process defining:

- Methods of data collection;
- Subjects who have access to the data;
- Method of transferring data to third parties;
- Methods of updating and deleting data;
- Methods of offering information to interested parties and collecting consent;
- Asset model to support the treatment;
- Maximum data retention period.

7.3.2 Define if a DPIA is needed

Thanks to preliminary risk assessment, information are available in order to evaluate if a DPIA is needed. It will happen in these three cases:

- 1) High risk detected;
- 2) Unsafe treatment;
- 3) Impact on one of nine criteria analyzed in the preliminary assessment.

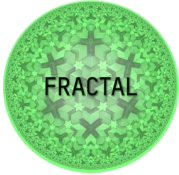
Here the explanation of these three cases.

7.3.2.1 High risk

The processing activity that is the subject of this impact assessment - given the nature, the objects, the contexts and the purposes of the processing - could present a high risk for the rights and freedoms of individuals according to the criteria set out in “Article 35, par. 3” of the GDPR 2016/679.

The treatment falls into the following two categories for which it is necessary to develop an impact assessment process based on the indications of the guideline WP248:

- sensitive data or data of highly personal nature;

	Project	FRACTAL	
	Title	FRACTAL Cybersecurity features and requirements for Fractal	
	Del. Code	D4.5	

- data relating to vulnerable data subjects (recital 75): the processing of this type of data may cause an imbalance of power between the data controller and the data subjects, who may not be able to consent or oppose the processing of their data or to exercise your rights.

7.3.2.2 Unsafe Treatment

Treatment is unsafe in one of this five situations:

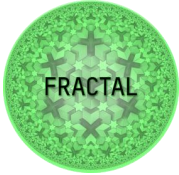
- there is no transparency of the treatment;
- data are not adequate, relevant and limited to what is necessary with respect to the purposes of the processing;
- data are inaccurate with respect to the purposes of the processing;
- data are stored for a time longer than necessary with respect to the purposes of the processing;
- when there is no integrity and confidentiality of the personal data being processed.

7.3.2.3 Impact on one of nine criteria analyzed in the preliminary assessment

The guidelines introduce nine criteria for assessing if and when to perform a DPIA, presented in the Table 12.

If at least one of the 9 criteria is part of the use case, a DPIA is required. The nine criteria were submitted to Use Cases within the questionnaire provided as first step of the workflow.

Table 12: List of Requirements

	Project	FRACTAL	
	Title	FRACTAL Cybersecurity features and requirements for Fractal	
	Del. Code	D4.5	

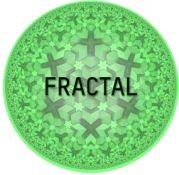
N.	REQUIREMENTS
1	Evaluation or scoring, including profiling and forecasting, in particular of "aspects concerning the performance of the data subject at work, economic situation, health, personal preferences or interests, reliability or behavior, position or movements".
2	Automated decisions with significant legal or similar effects: processing that aims to make decisions on data subjects, which produce "legal effects on the natural person" or "significantly affect the natural person" (Article 35 (3) (a)).
3	Systematic monitoring: processing used to observe, monitor, or control data subjects, including data collected via networks or "systematic monitoring of a publicly accessible area" (Article 35 (3) (c)). This type of monitoring is a criterion as personal data may be collected in circumstances where data subjects may not be aware of who collects their data and how it will be used.
4	Sensitive data or data of a highly personal nature: these include special categories of personal data as defined in Article 9 (for example information on the political opinions of individuals), as well as personal data relating to criminal sentences or offenses referred to in Article 10.
5	Data processed on a large scale: the GDPR does not define what is meant by 'large scale', although recital 91 provides some indications. In any case, WP29 recommends considering the following factors in particular to determine if the treatment is performed on a large scale:
6	Correspondence or combination of data sets, for example from two or more processing operations, performed for different purposes and / or by data holders deriving from the subject in order to go beyond expectations.
7	Data relating to vulnerable individuals (recital 75): The processing of this type of data falls under the criteria due to the increased power imbalance between data subjects and the controller, which means that individuals may not be in able to allow or easily oppose the processing of their data or to exercise their rights.
8	Innovative use or application of new technological or organizational solutions, such as combining the use of facial recognition and fingerprinting for better physical access control, etc. The GDPR clarifies (Article 35, paragraph 1, and recitals 89 and 91) that the use of a new technology, defined as "compliant with the state reached by technological knowledge" (recital 91), may involve the need to perform a DPIA.
9	When the processing itself "prevents data subjects from exercising a right or from using a service or a contract" (article 22 and recital 91). This includes processing operations that aim to allow, modify or refuse data subjects' access to a service or to enter into a contract.

7.3.3 Method of conducting the DPIA

The purpose of the activity is to collect all the information necessary for the first assessment about whether the data treatment complies with the GDPR regulation or not and to understand whether that treatment must be subjected to a DPIA assessment or not.

This document mainly includes:

- A systematic description of the intended processing and of the purposes of the processing;

	Project	FRACTAL	
	Title	FRACTAL Cybersecurity features and requirements for Fractal	
	Del. Code	D4.5	

- An assessment of the necessity and proportionality of the processing in relation to the purposes;
- An assessment of the risks to the rights and freedoms of the data subjects;
- The measures envisaged to address the risks, including guarantees, security measures and mechanisms to guarantee the protection of personal data and demonstrate compliance with the Regulation, taking into account the rights and legitimate interests of the data subjects.

The DPIA will be conducted by interns within the project organization. The data controllers are those who establish the purposes and methods of the processing of personal data.

7.4 Preliminary assessment

In this section the preliminary risk assessment will be presented for each Use Case in a dedicated subsection.

7.4.1 Use case 1: Engineering & maintenance works

7.4.1.1 STEP 1 - Description of the treatment

Stakeholders

The stakeholders involved are the construction companies, which will receive an analysis of the generated data, and the subcontractors of the work sites, which will generate the information.

Purpose of the treatment

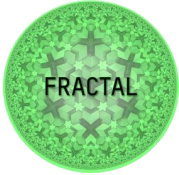
Each demonstrator has a different objective, but the main goal is the same, the reduction of risks within construction works and supervision / maintenance tasks.

- Demo 1: The objective is the detection of cracks in the surface of concrete structures, such as bridges or viaducts.
- Demo 2: The objective is to improve occupational safety and health in the construction works.

Description of the treatment and information flows

Demo 1: The information is collected by an UAV operated by a technical assistance operator. The images will be sent to a hardware platform to be processed by an AI algorithm.

Demo 2: The information is collected by a wireless sensor network (WSN) composed by small devices, which information is stored in a remote repository. The information

	Project	FRACTAL	
	Title	FRACTAL Cybersecurity features and requirements for Fractal	
	Del. Code	D4.5	

will be provided by the owners of the devices frequently to Indra and Zylk. Then the information will be analyzed.

Data object of the treatment

The treatment is performed for obtaining the expected results such as the images where the cracks in concrete structures are represented (Demo 1), and the proximity alarms between construction workforce and the machinery, apart from other data as the date and time of the alarm, subject and machine that generates the alarm, location of the machine, etc. (Demo 2).

Method of treatment

The Versal platform (VCK190) will be used for the inference of the algorithm for detecting the cracks in Demo 1. For Demo 2, the data will be used for the prediction of alarms of proximity through an algorithm developed by Zylk. Data will also be integrated in a IoT platform for the visualization of the information collected.

Operations performed

Demo 1

- Development of an AI algorithm capable to identify small cracks on the surface.
- Process of UAV images in the Versal Platform (VCK190).
- Creation of a quick cracks map to be supervised by an expert and performing an accurate supervision and maintenance only in those cracks that apparently can be a problem for the security of the structure.

Demo 2


- Collection of the proximity alarms between the construction workforce and the machinery that could be a risk for the personnel.
- Predict future risks on field based on the data collected and the work environment using the Versal Platform.
- Redistribute the machinery movements on site.

Data processed storage

Demo 1: The data processed will be stored in a local folder.

Demo 2: The data collected will be stored in a database in the Fractal node during the time necessary for their treatment.

Business processes involved in the treatment

	Project	FRACTAL	
	Title	FRACTAL Cybersecurity features and requirements for Fractal	
	Del. Code	D4.5	

Demo 1: IFT receive the images collected by UAV and it processes the data. Prointec (Structures Department) receives the data processed with the cracks detected and an expert analyzes the result.

Demo 2: Indra, Prointec and Zylk.

7.4.1.2 STEP 2 - Conformity assessment

Methods of data collection

Demo 1: The data must not be transferred to third parties, only those parties which are part of the treatment can access to it. As the data is stored in a local folder, it is not necessary to encrypt them.

Demo 2: The data is stored in a database in the Fractal node for the time necessary for their treatment. After processing and inference from the ML models, the results and the raw data are sent to the IoT platform where they are stored for historical data collection purposes. For memory and resource constraints in the Fractal platform, raw data are removed after being processed.

Subjects who have access to the data

Demo 1: Indra, IFT and Prointec can access to the data.

Demo 2: Indra, Prointec, Zylk and the device owners can access the data.

Method of transferring data to third parties

Dem 1: There is no possibility of data transfer to third parties.

Dem 2: Data transfer to third parties is not possible in demo 2.

Methods of updating and deleting data

The data must not be modified during the treatment and must be deleted when the treatment is finished.

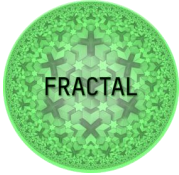
Methods of offering information to interested parties and collecting consent

Dem 2: Since the sensors are wearables, people who will carry the sensors must have given their permission. They will be informed that the ones they carry do not have GPS location that they only serve to calculate distances to the construction machinery.

Asset model to support the treatments

Business hardware, software, archives, networks, and platforms.

Maximum data retention period

	Project	FRACTAL
	Title	FRACTAL Cybersecurity features and requirements for Fractal
	Del. Code	D4.5

The maximum data retention period must be equal to the duration of the treatment.

7.4.2 Use Case 2: Automotive Air Control

7.4.2.1 STEP 1 - Description of the treatment

Stakeholders

Stakeholders are automotive engineers who are processing the data resulting from simulation and data resulting from test drives.

Purpose of the treatment

Develop an AI-based control strategy using the plant model for the target configuration alongside with the rule-based control strategy to achieve the defined calibration targets.

Description of the treatment and information flows

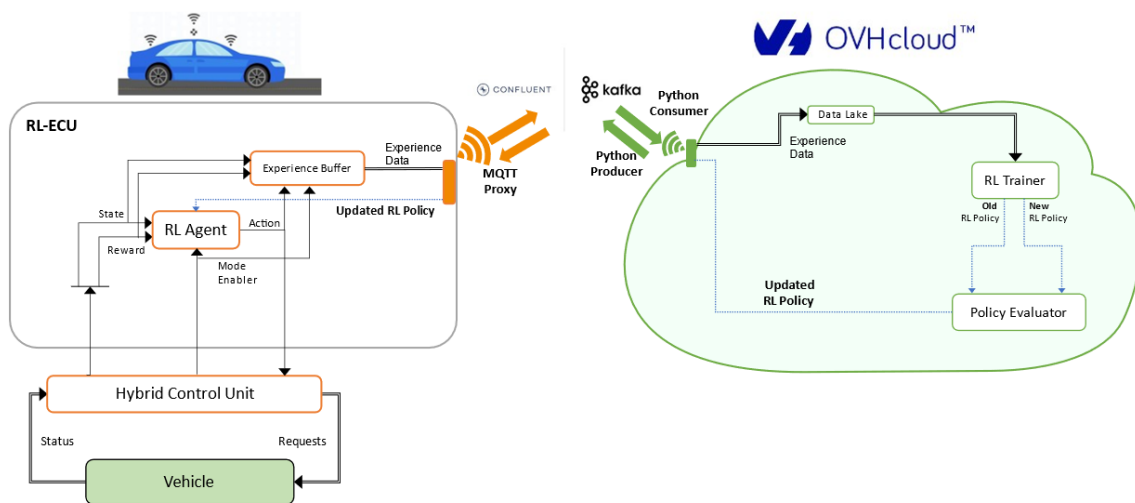


Figure 8: Treatment flow for UC2

The agent on the car is simulated using a development board (one of the FRACTAL nodes).

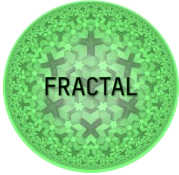
Data object of the treatment

Data resulting from plant model simulation.

Method of treatment

With the help of electronic tools.

Operations performed

	Project	FRACTAL	
	Title	FRACTAL Cybersecurity features and requirements for Fractal	
	Del. Code	D4.5	

Train initial model on the cloud, have 2 to 3 validation drive cycles in laptop or edge, stream through the validation drive cycles, have online inference of the model on the edge (laptop), store the experience buffer to OVH S3 by streaming, trigger re-training on the cloud, evaluate models, send updated model back to the edge.

Data processed storage // Conservation of processed data

The processed data are stored locally (permanent storage) and in OVH cloud environment (for the duration of treatment). Executable ML-model is deployed to a FRACTAL node (for the duration of treatment).

Business processes involved in the treatment

AVL engineers implement a workflow that requires a dedicated cloud provider (OVH cloud) and the provider of edge infrastructure (PLC2).

7.4.2.2 STEP 2 - Conformity assessment

Methods of data collection

Data are stored within AVL premises and on OVH cloud.

Subjects who have access to the data

Dedicated AVL engineers have access to the data.

Method of transferring data to third parties

The data must not be transferred to third parties, only those who are part of the treatment can access.

Methods of updating and deleting data

The data must not be modified during the treatment and must be deleted when the treatment is finished (OVH cloud, FRACTAL node).

Methods of offering information to interested parties and collecting consent

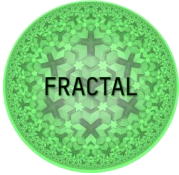
No personal data are collected and no consent is needed.

Asset model to support the treatments

Business hardware, software, archives, networks, and platforms.

Maximum data retention period

The maximum data retention period must be equal to the duration of the treatment.

	Project	FRACTAL	
	Title	FRACTAL Cybersecurity features and requirements for Fractal	
	Del. Code	D4.5	

7.4.3 Use case 3: Smart meter

7.4.3.1 STEP 1 – Description of the treatment

Stakeholders

For future scope, the company that owns the device. Not in FRACTAL project scope.

Purpose of the treatment

The aim is to read the meters remotely by connecting them to the Internet. This allows utility providers to remotely read meters with the advantage that they would no longer need to visit customers to physically read the meters.

Description of the treatment and information flows

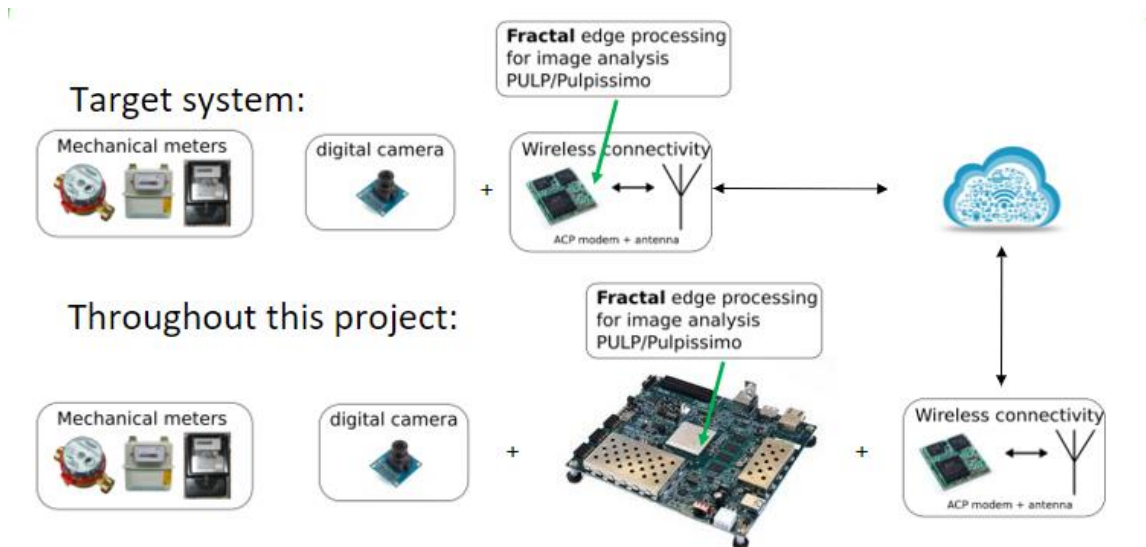


Figure 9: Treatment flow for UC3

Data object of the treatment

No real data is collected during the project, only sample data. In its final form, once deployed, the device will collect real meter data.


Method of treatment

With the help of electronic tools.

Operations performed

A picture is analyzed to extract the meter stand. The resulting number is stored as a number.

Data processed storage

	Project	FRACTAL	
	Title	FRACTAL Cybersecurity features and requirements for Fractal	
	Del. Code	D4.5	

Data is stored encrypted on the device until it is successfully transmitted to the utility provider.

Business processes involved in the treatment

ACP, ETH.

7.4.3.2 STEP 2 – Conformity assessment

Methods of data collection

This data is stored encrypted on the device and sent encrypted to the service provider.

Subjects who have access to the data

No other companies/users can access the data.

Method of transferring data to third parties

The data must not be transferred to third parties, only those who are part of the treatment can access.

Methods of updating and deleting data

The data must not be modified during the treatment and must be deleted when the treatment is finished.

Methods of offering information to interested parties and collecting consent

A signed consent sheet is necessary at the beginning of the processing if the data used relate to personal data (i.e. if it is possible to identify the meter owner, but it is not in project scope).

Asset model to support the treatments

Business hardware, software, archives, networks, and platforms.


Maximum data retention period

The maximum data retention period must be equal to the duration of the treatment.

7.4.4 Use Case 4: Low-latency Object Detection as a generic building block for perception in the edge for industrial application

7.4.4.1 STEP 1 - Description of the treatment

Stakeholders

	Project	FRACTAL	
	Title	FRACTAL Cybersecurity features and requirements for Fractal	
	Del. Code	D4.5	

UC4 represents a system solution in form of generic building block for vision-based object detection. Computer vision is a crucial component for cognitivity to extract meaningful information from the surrounding. The use of Convolutional Neural Network (CNN) has shown impressive results on accuracy for object detection.

Purpose of the treatment

The aim is processing images in real-time with low latency prediction.

Description of the treatment and information flows

Formatting input image size, rearranging image layout, fragmenting the image frame, configuring HWA, transferring the image fragment and weights from system memory to HWA local memory, start the convolution, transferring the image fragment from HWA local memory to system memory, postprocessing of image, display the results.

Data object of the treatment

A set of photos from printed circuit boards.

Method of treatment

With the help of electronic tools.

Operations performed

Formatting input image size, rearranging image layout, fragmenting the image frame, configuring HWA, transferring the image fragment and weights from system memory to HWA local memory, start the convolution, transferring the image fragment from HWA local memory to system memory, postprocessing of image, display the results.

Data processed storage

A set of photos are collected and stored locally.

Business processes involved in the treatment

Siemens AG and ETH Zürich.

7.4.4.2 STEP 2 - Conformity assessment

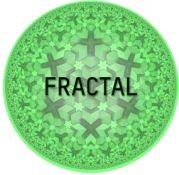
Methods of data collection

Data are not collected or stored.

Subjects who have access to the data

Data accessible only by the team involved in the treatment

Method of transferring data to third parties

	Project	FRACTAL	
	Title	FRACTAL Cybersecurity features and requirements for Fractal	
	Del. Code	D4.5	

The data must not be transferred to third parties, only those who are part of the treatment can access.

Methods of updating and deleting data

The data must not be modified during the treatment and must be deleted when the treatment is finished.

Methods of offering information to interested parties and collecting consent

No personal data collected. No consent needed.

Asset model to support the treatments

Business hardware, software, archives, networks, and platforms.

Maximum data retention period

The maximum data retention period must be equal to the duration of the treatment.

7.4.5 Use case 5: Increasing the safety of autonomous train through AI techniques

7.4.5.1 STEP 1 – Description of the treatment

Stakeholders

Videos during the operation of the night train, accessible only to members of the team involved in the treatment.

Purpose of the treatment

The aim is to apply CV&AI techniques to improve the different functionalities of autonomous train operation, such as precision stopping, visual odometry, rolling stock coupling operation or detection-identification of people and obstacles in railways.

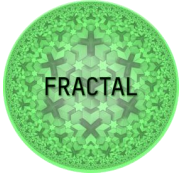
Description of the treatment and information flows

The recorded videos are used to validate the final build of the fractal system for the use case that simulates the actual input. This evaluation leads to numerical results for benchmarking and KPIs. Eventually some single images or videos can be used for demonstration purposes without showing any person or personal information.

Data object of the treatment

Videos during night train operation.

Method of treatment

	Project	FRACTAL	
	Title	FRACTAL Cybersecurity features and requirements for Fractal	
	Del. Code	D4.5	

With the help of electronic tools.

Operations performed

Data labelling for AI training. Inference during evaluation.

Data processed storage

Permanent stored.

Business processes involved in the treatment

CAF is the data controller and will be responsible for the processing.

7.4.5.2 STEP 2 – Conformity assessment

Methods of data collection

Videos are stored on CAF's non-public servers.

Subjects who have access to the data

Data is only accessible by team members, involved in the treatment.

Method of transferring data to third parties

It can be transferred under confidentiality legal agreements.

Methods of updating and deleting data

The data must not be modified during the treatment and must be deleted when the treatment is finished.

Methods of offering information to interested parties and collecting consent

A signed consent sheet is necessary at the beginning of the processing if the data used relate to personal data.

Asset model to support the treatments

Business hardware, software, archives, networks, and platforms.

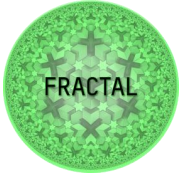
Maximum data retention period

Permanent stored.

7.4.6 Use Case 6: Intelligent Totem – Elaborate data collected using heterogeneous technologies

7.4.6.1 STEP 1 - Description of the treatment

Stakeholders

	Project	FRACTAL	
	Title	FRACTAL Cybersecurity features and requirements for Fractal	
	Del. Code	D4.5	

Consumers and resellers of retail products.

Purpose of the treatment

The overall aim is to maximize the impact of personalized advertisements and product recommendations by prompting customers to purchase products.

Description of the treatment and information flows

The totem will be equipped with several sensors that provide information to be processed using its AI-based processing unit. There are 4 phases:

Phase 1: Data acquisition

Phase 2: Network training

Phase 3: Real-time detection

Phase 4: Alarm triggering and sending

Data object of the treatment

The data collected are images and / or audio that are used to collect the sex, age and language of users. From the images collected it is also possible to count the people near the totem, calculate the heat map, detect the intensity and variation of the crowd and detect (pleasant to have) the level of attention.

Method of treatment

With the help of electronic tools.

Operations performed

Collection, registration, organization, storage, extraction, consultation, use, limitation, processing with ETL modality and AI processing.

Data processed storage

The data are not stored.

Business processes involved in the treatment

AITEK, UNIVAQ, MODIS, UNIMORE, UNIGE, RULEX e RO TECHNOLOGY.

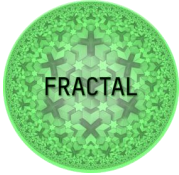
7.4.6.2 STEP 2 - Conformity assessment

Methods of data collection

The data are not stored in any archive.

Subjects who have access to the data

The data are not stored. For this reason, no one is able to access the data.

	Project	FRACTAL	
	Title	FRACTAL Cybersecurity features and requirements for Fractal	
	Del. Code	D4.5	

Method of transferring data to third parties

The data are not transferred to third parties because the data are not stored and there is no possibility to transfer it.

Methods of updating and deleting data

The data are not changed because the data are not stored and there is no possibility to change it later. The data are immediately deleted without being archived.

Methods of offering information to interested parties and collecting consent

A signed consent sheet is necessary at the beginning of the processing, if the data used relate to personal data.

As there is no possibility to identify people and there is no data collection, consent is not needed.

Asset model to support the treatments

Business hardware, software, archives, networks, and platforms.

Maximum data retention period

Data are immediately deleted.

7.4.7 Use case 7: Autonomous SPIDER robot

7.4.7.1 STEP 1 – Description of the treatment

Stakeholders

Stakeholders are the members of the development team, implementing functions of UC7.

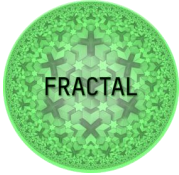
Purpose of the treatment

Data is collected to develop and test the functions implemented with UC7; namely the collision avoidance function and the path tracking function.

Description of the treatment and information flows

1. Data is collected while test drives at the robot.
2. Stored data is transferred to a local server with access for developers.
3. Stored data is used for training models, and evaluation of functions.

Data object of the treatment

	Project	FRACTAL	
	Title	FRACTAL Cybersecurity features and requirements for Fractal	
	Del. Code	D4.5	

The stored data is composed of diagnosis data of the executed functions, localization of the robot (positioning), and 3D point clouds. All of those data are labelled with timestamps.

Method of treatment

With the help of electronic tools.

Operations performed

Collection, registration, organization, storage, consultation, use, and AI processing.

Data processed storage

Permanently stored locally.

Business processes involved in the treatment

Virtual Vehicle Research GmbH.

7.4.7.2 STEP 2 – Conformity assessment

Methods of data collection

Recorded data is stored on Virtual Vehicles non-public servers.

Subjects who have access to the data

Data is accessible only to team members working on the development of UC7 functions.

Method of transferring data to third parties

The data must not be transferred to third parties, only those who are part of the treatment can access.

Methods of updating and deleting data

The data must not be modified during the treatment and must be deleted when the treatment is finished.

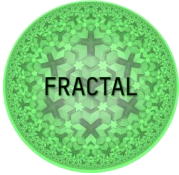
Methods of offering information to interested parties and collecting consent

The are no personal data, so consent is not needed.

Asset model to support the treatments

Business hardware, software, archives, networks, and platforms.

Maximum data retention period

	Project	FRACTAL	
	Title	FRACTAL Cybersecurity features and requirements for Fractal	
	Del. Code	D4.5	

The maximum data retention period must be equal to the duration of the treatment.

7.4.8 Use case 8: Shuttle for moving goods in a warehouse

7.4.8.1 STEP 1 - Description of the treatment

Stakeholders

The company BEEWEN Automation GmbH is the sole stakeholder of the treatment.

Purpose of the treatment

The purpose of the treatment is to improve warehouse productivity.

Description of the treatment and information flows

The treatment can be divided into 4 steps

1. Detection of human body;
2. Calculate distance;
3. Evaluation process for relative distance between shuttle and human body;
4. Give output to safety plc.

Data object of the treatment

Camera stream or single images of the stream for data processing.

Method of treatment

With the help of electronic tools.

Operations performed

Collection: labeling and storing on local memory


Evaluation: ai model processing, distance calculation, evaluation process

Data processed storage

For development purposes, data will be collected locally only in the test setup.

Later it is planned, that during a project at the ramp-up phase data could be acquired, when the environment changes very much in terms of light conditions or other properties.

Business processes involved in the treatment

	Project	FRACTAL	
	Title	FRACTAL Cybersecurity features and requirements for Fractal	
	Del. Code	D4.5	

BEEA - Development of the concatenation between the object detection and the safety service.

7.4.8.2 STEP 2 - Conformity assessment

Methods of data collection

Non-public servers of the company for internal purposes of the R&D department.

Subjects who have access to the data

R&D and software department of the company.

Method of transferring data to third parties

The data must not be transferred to third parties, only those who are part of the treatment can access.

Methods of updating and deleting data

The data must not be modified during the treatment and must be deleted when the treatment is finished.

Methods of offering information to interested parties and collecting consent

A signed consent sheet is necessary at the beginning of the processing, if the data used relate to personal data, but not foreseen for project scope.

Asset model to support the treatments

Business hardware, software, archives, networks, and platforms.

Maximum data retention period

The maximum data retention period must be equal to the duration of the treatment.

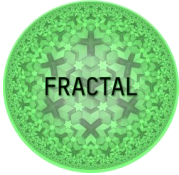
7.5 Data confidentiality measures

After preliminary risk assessment and before to evaluate if a DPIA is needed for each Use Case, it is important to mention some important concepts about:

- Data confidentiality measures;
- Rights of interested parties;
- Principles and rights treatment has to respect.

Here some example of security measures to guarantee data confidentiality / to prevent unauthorized or illegitimate processing of personal data.

Organizational, such as: internal instructions; assignment of offices; training of employees; data classification; controlled destruction of media.

	Project	FRACTAL	
	Title	FRACTAL Cybersecurity features and requirements for Fractal	
	Del. Code	D4.5	

Periodic updating of the processing areas allowed to the persons in charge or to the physical organizational units, such as: supervision of the data custody offices; custody in inaccessible filing cabinets or cabinets; fire-fighting devices; continuity of power supply.


Verification of the readability of the logical supports, such as: identification of the person in charge and / or the user; access control to data and programs; updated antivirus checks; continuous monitoring of work sessions; control of the supports delivered for maintenance

For details, please refer to the Data Processing Register, art. 5 and 6.

The interested party has the right to ask the data controller to access personal data, correct or delete them, limit the processing; can also oppose the processing and exercise the right to the portability of the data provided and processed automatically, with the consent of the interested party or on the basis of a contract between the parties. The rights referring to personal data concerning deceased persons can be exercised by those who have an interest of their own, or act to protect the person concerned, as his agent, or for family reasons worthy of protection. It is the right of the interested party to lodge a complaint against the data processing carried out by the Company to the competent Supervisory Authority (Guarantor for the protection of personal data), or appeal to the Judicial Authority.

Treatment has to respect:

- the principles of lawfulness, correctness, and transparency;
- the principle of purpose limitation;
- the principle of data minimization;
- the principle of data accuracy;
- the principle of limitation of data retention;
- the right to information;
- the right to access data;
- the right of portability;
- the right of rectification;
- the right of cancellation (right to be forgotten);
- the right to limit the processing;
- the right to object to the processing.

	Project	FRACTAL	
	Title	FRACTAL Cybersecurity features and requirements for Fractal	
	Del. Code	D4.5	

7.6 Conduct the DPIA?

In this section results from preliminary risk assessment will be evaluated taking into account the questionnaire provided to each Use Case at the beginning and the nine criteria of mentioned guidelines.

7.6.1 Use case 1: Engineering & maintenance works


After filling in the report, the following emerged:

Table 13: Part of Questionnaire for UC1

REQ ID	REQUIREMENTS	YES/NO	Why YES? (describe the data treatment)
1	Evaluation or scoring, including profiling and forecasting, in particular of "aspects concerning the performance of the data subject at work, economic situation, health, personal preferences or interests, reliability or behavior, position or movements".	Yes	UC1 DEM2: Data on the relative position of the workers in a construction site with respect to the machinery are handled.
7	Data relating to vulnerable individuals (recital 75): The processing of this type of data falls under the criteria due to the increased power imbalance between data subjects and the controller, which means that individuals may not be in able to allow or easily oppose the processing of their data or to exercise their rights.	NO.	UC1 DEM2: Since the sensors are wearables, people who will carry the sensors must have given their permission. They will be informed that the ones they carry do not have GPS location that they only serve to calculate distances to the construction machinery.

Since there are requirements 1 and 7 for this use case, it can be argued that the DPIA is necessary. However, in demonstrator 1 the data are videos or images related to cracks in concrete structures and in demonstrator 2 is data collected on interactions between construction workers and machinery, but never personal information on workers.

In light of these considerations, it is believed that any risks can be considered substantially overall **acceptable**.

	Project	FRACTAL	
	Title	FRACTAL Cybersecurity features and requirements for Fractal	
	Del. Code	D4.5	

7.6.2 Use case 2: AI-based control strategies (air path, thermal mgmt.)

The results of the survey conducted above do not highlight the existence of risks that damage the rights and freedoms of individuals, since in the compilation of the report there is no evidence of any of the 9 criteria and the data used for the processing are not given sensitive data attributable to personal data of natural persons. In light of these considerations, it is believed that any risks can be considered as substantially **non-existent** overall.

7.6.3 Use case 3: Smart meters for everyone

The results of the survey conducted above do not highlight the existence of risks that damage the rights and freedoms of individuals, since in the compilation of the report there is no evidence of any of the 9 criteria and the data used for the processing are not given sensitive data attributable to personal data of natural persons. In light of these considerations, it is believed that any risks can be considered as substantially **non-existent** overall.

7.6.4 Use Case 4: Low- latency Object Detection in Industry 4.0


The results of the survey conducted above do not highlight the existence of risks that affect the rights and freedoms of individuals, since in the compilation of the report there is no evidence of any of the 9 criteria and the data used for the treatment are not sensitive data attributable to personal data of natural persons. The only data analyzed concern a series of photos from printed circuits to locate objects through images, without the presence of people. In light of these considerations, it is believed that any risks can be considered as substantially **non-existent** overall.

7.6.5 Use case 5: Autonomous train operation

The results of the preliminary assessment conducted above, according to the Fractal project scope, do not highlight the existence of risks that harm people's rights and freedoms, since in the compilation of the report there is no evidence of any of the 9 criteria and the only ones the data analyzed relates to video during the night traffic of trains. Eventually some single images or videos can be used for demonstration purposes without showing any person or personal information, the only videos where people could appear are videos taken from YouTube. When it is implemented in the station in the future there may be photos and / or videos where there are people. In light of these considerations, it is believed that any risks can be considered as substantially **non-existent** overall for project scope, but it is believed that any risks can be considered substantially overall **acceptable**.

7.6.6 Use case 6: Intelligent totem

The results of the investigation conducted above do not highlight the existence of risks that harm people's rights and freedoms, as the data collected are immediately deleted without the possibility of being archived and reused. In this way there are no risks to the rights and freedoms of individuals. In light of these considerations, it is believed that any risks can be considered as substantially **non-existent** as a whole.

	Project	FRACTAL	
	Title	FRACTAL Cybersecurity features and requirements for Fractal	
	Del. Code	D4.5	

7.6.7 Use case 7: SPIDER autonomous robot

The results of the preliminary assessment conducted above do not highlight the existence of risks having an impact on the rights and freedoms of individuals, since in the compilation of the report there is no evidence of any of the 9 criteria and the data used for the processing are not sensitive data attributable to personal data of individuals. In light of these considerations, it is believed that any risks can be considered substantially **non-existent** as a whole.

7.6.8 Use case 8: Shuttle in Warehouse Systems

The results of the preliminary assessment conducted above do not highlight the existence of risks having an impact on the rights and freedoms of individuals, since in the compilation of the report there is no evidence of any of the 9 criteria and the data used for the processing are not sensitive data attributable to personal data of individuals. In light of these considerations, it is believed that any risks can be considered substantially **non-existent** as a whole.

7.7 DPIA EXECUTION

After preliminary risk assessment it was evaluated that only Use Case 1 require a DPIA execution.

7.7.1 Phase 1 for all use cases

Phase 1 - Additional information for risk analysis

In addition to what has already been stated in the preliminary assessment, to which reference should be made.

Used technologies

No new information technologies will be used that could have a significant potential for breaching the protection of personal data and reducing the level of data protection, which must be guaranteed to the data subjects.

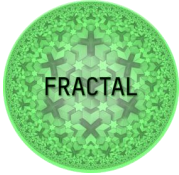
Identification methods

No new methods of data identification will be used, but already existing and in use identifiers will be reused.

No new or significantly modified identity authenticity requirements will be used, which can be intrusive or burdensome.

Changes to the methods of data processing

The treatment initiative will not bring about new or significant changes to the methods of processing personal data, which could give rise to concerns in the interested party.

	Project	FRACTAL	
	Title	FRACTAL Cybersecurity features and requirements for Fractal	
	Del. Code	D4.5	

Personal data relating to the data subject, already present in an existing database, will not be subjected to new or modified methods of treatment.

The treatment initiative will not bring about new or significant changes to the methods of consolidation, interchange, cross-references, matching of personal data, coming from multiple processing systems.

Changes to data processing procedures

The processing may not introduce new methods and procedures for data collection, which are not sufficiently transparent or are intrusive, nor changes to systems and processes, supported by regulations in force, which may have unclear or unsatisfactory results, or which modify the level of data security, so as to lead to unclear or unsatisfactory results.

The processing may not introduce new or modified secure procedures for accessing data or methods of communication and consultation, which may be unclear or permissive.

The processing will not introduce new or modified methods of data retention, which may be unclear or extremely prolonged.

Exemptions from the application of the provisions of the regulation

The processing activity does not go beyond the scope of the legislative provisions of the European Union, is not carried out by a natural person exclusively for personal and family purposes and is not carried out by public authorities for the purpose of prevention, investigation, identification, and prosecution of crimes or in order to apply penalties.

7.7.2 Phase 2 for use cases that require DPIA (only UC1)

Phase 2 - Risk Assessment

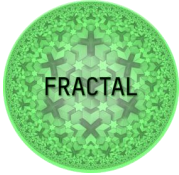
7.7.2.1 Evaluation methodology

Risk analysis is a process for identifying and assessing the damage caused by threats and vulnerabilities in combination on one or more specific corporate assets. It also serves to justify countermeasures, to assess that they are effective, of reasonable cost, effectively applicable to the context and able to respond to threats in time. This analysis aims to minimize the probability of risks occurring and the impacts that possible violations of personal data could entail on individuals, as summarized by way of example.

Risks: destruction, loss, modification, unauthorized disclosure, or unauthorized access to personal data.

Impact:

- from violation of physical security;

	Project	FRACTAL	
	Title	FRACTAL Cybersecurity features and requirements for Fractal	
	Del. Code	D4.5	

- from violation of identification data or relating to identity personal;
- material (financial or asset losses);
- moral or biological (disturbance due to the dissemination of confidential information, compromise of a state of health, event harmful to human rights or the integrity of the person);
- social (discriminatory consequences, loss of autonomy);

The DPIA is based on a risk analysis centered on:

- risks deriving from the intrinsic content of the treatment;
- risks deriving from possible security breaches.

In relation to the possible applicable controls, thus obtaining a **“normalized” risk index** with respect to the company context.

The normalized risk RN is calculated according to the following 3 factors.

$$RN = f(P, C, V)$$

where:

P = probability (estimate of the probability of occurrence of the events causing the loss, violation, uncontrolled distribution of data = dangers)

C = consequences generated by the event (estimate of the severity of the expected damage with respect to the occurrence of a certain event)

V = vulnerability with respect to the degree of adequacy of the measures (degree of adequacy of the measures that counteract the occurrence of events)

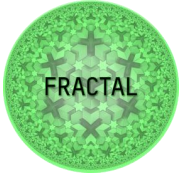
First, **the intrinsic risk Ri** is derived as a product of probability P and consequences C, based on the numerical indices assigned to both factors.

Table 14: Probability values

PROBABILITY	
1	Unlikely
2	Not very likely
3	Likely
4	Almost certain

Consequences C is associated with a numerical index represented in the Table 15:

Table 15: Consequences values

	Project	FRACTAL	
	Title	FRACTAL Cybersecurity features and requirements for Fractal	
	Del. Code	D4.5	

CONSEQUENCES	
1	Negligible
2	Marginal
3	Limited
4	Serious

The matrix resulting from the combination of probability and consequences is represented in the Table 16:

Table 16: Matrix combination of probability and consequences

PROBABILITY	4	4	8	12	16
	3	3	6	9	12
	2	2	4	6	8
	1	1	2	3	4
RI = P x C		1	2	3	4
		CONSEQUENCES			

The intrinsic risk is derived by considering all possible hazards and risks.

Table 17: Intrinsic Risk values

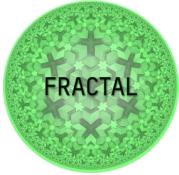
INTRINSIC RISK	
Ri = P x C	Reference values
Very low	(1 ≤ Ri ≤ 2)
Low	(3 ≤ Ri ≤ 4)
Relevant	(6 ≤ Ri ≤ 9)
High	(12 ≤ Ri ≤ 16)

To derive the RN Normalized Risk, the vulnerability factor is introduced which provides an indication about the adequacy of the safety measures implemented for each risk.

Vulnerability V is associated with a numerical index represented in the Table 18:

Table 18: Vulnerability values

VULNERABILITY		VALUE
1	Adequate	0.25

	Project	FRACTAL	
	Title	FRACTAL Cybersecurity features and requirements for Fractal	
	Del. Code	D4.5	

2	Partially adequate	0.5
3	Inadequate	1

For each risk, the safety measures adopted are indicated and the degree of adequacy is defined, assigning one of the possible values:

- 0.25
- 0.5
- 1

To derive the value of the normalized risk RN, the intrinsic risk Ri is multiplied with the worst value assigned to the safety measures relative to that risk.

Table 19: Matrix combination of vulnerability and intrinsic risk

VULNERABILITY	1	$1 < RN \leq 2$	$3 < RN \leq 4$	$6 < RN \leq 9$	$12 < RN \leq 16$
	0.5	$0.5 < RN \leq 1$	$1.5 < RN \leq 2$	$3 < RN \leq 5$	$6 < RN \leq 8$
	0.25	$0.25 < RN \leq 0.5$	$0.75 < RN \leq 1$	$1.5 < RN \leq 3$	$3 < RN \leq 4$
RN		$1 < Ri \leq 2$	$3 < Ri \leq 4$	$6 < Ri \leq 9$	$12 < Ri \leq 16$
INTRINSIC RISK					

Table 20: Normalized risk values

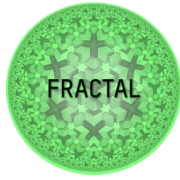
NORMALIZED RISK	
RN=RI x V	Value
Very low	$0,25 \leq RN \leq 1$
Low	$1 \leq RN \leq 3$
Relevant	$3 \leq RN \leq 9$
High	$9 \leq RN \leq 16$

7.7.2.2 Definition of danger areas, generated risks, and assessment of the intrinsic risk level

In Table 21 there is the breakdown of the main danger areas with the risks generated, and the relative estimates on the probability of occurrence and consequences.

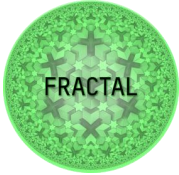
Table 21: List of danger, risks, probability and consequences

DANGERS	RISKS	Estimated PROBABILITY	CONSEQUENCES estimated
---------	-------	-----------------------	------------------------



Project	FRACTAL	
Title	FRACTAL Cybersecurity features and requirements for Fractal	
Del. Code	D4.5	

Physical agents (fire, flood, external attacks)	<ul style="list-style-type: none"> • Damage • Lost • Unauthorized destruction 	Not very likely	Serious
Natural events (earthquakes, volcanic eruptions, etc.)	<ul style="list-style-type: none"> • Damage • Lost • Unauthorized destruction 	Unlikely	Serious
Interruption of services (power surges, air conditioning system failures, interruption of network connections, etc.)	<ul style="list-style-type: none"> • Damage • Lost • Unauthorized destruction 	Not very likely	Limited
Technical problems (software anomalies and malfunctions, hardware problems or IT service components)	<ul style="list-style-type: none"> • Damage • Lost • Unauthorized destruction • Unauthorized data access 	Likely	Serious
Information compromise	<ul style="list-style-type: none"> • Damage • Lost • Unauthorized destruction 	Not very likely	Serious
(wiretapping, disclosure, information, infiltration into e-mail messages, etc.)	<ul style="list-style-type: none"> • Damage • Lost • Unauthorized destruction • Unauthorized data access 	Not very likely	Serious

	Project	FRACTAL	
	Title	FRACTAL Cybersecurity features and requirements for Fractal	
	Del. Code	D4.5	

	<ul style="list-style-type: none"> • Unauthorized treatment • Treatment not in accordance with the purpose of the collection or illegal 		
--	---	--	--

Intrinsic risk (assessed on the basis of the average of the worst values of probability and consequence estimated for specific risk).

Table 22: Risk 1 with consequences and level of risk

RISK: Damage / Loss / Unauthorized Destruction		
PROBABILITY	CONSEQUENCES	LEVEL OF RISK
Not very likely	Serious	Relevant

Table 23: Risk 2 with consequences and level of risk

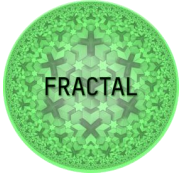
RISK: Unauthorized access		
PROBABILITY	CONSEQUENCES	LEVEL OF RISK
Not very likely	Serious	Relevant

Table 24: Risk 3 with consequences and level of risk

RISK: Unauthorized treatment		
PROBABILITY	CONSEQUENCES	LEVEL OF RISK
Not very likely	Serious	Relevant

Table 25: Risk 4 with consequences and level of risk

RISK: Treatment not in accordance with the purpose of the collection or illegal		
PROBABILITY	CONSEQUENCES	LEVEL OF RISK
Not very likely	Serious	Relevant

	Project	FRACTAL	
	Title	FRACTAL Cybersecurity features and requirements for Fractal	
	Del. Code	D4.5	

CONSEQUENCES AND PROBABILITY TABLE

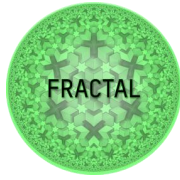
Table 26: Calculation of Intrinsic risk

TYPE OF RISK	RI=P x C	VALUE
Physical agents	2 x 4 = 8	RELEVANT (6≤Ri≤9)
Natural events	1 x 4 = 4	LOW (3≤Ri≤4)
Service interruption	2 x 3 = 6	RELEVANT (6≤Ri≤9)
Technical Problems	3 x 4 = 12	HIGH (9≤Ri≤16)
Information Commission	2 x 4 = 8	RELEVANT (6≤Ri≤9)
Unauthorized actions	2 x 4 = 8	RELEVANT (6≤Ri≤9)

7.7.2.3 Assessment of the suitability of technical and organizational security measures to make the risk acceptable

Table 27: Risks, measures and suitability

RISKS	MEASURES	SUITABILITY
Unauthorized damage / loss / destruction of personal data	making backup copies, saving, weekly data, periodic centralized backup,	ADEQUATE
Unauthorized access to personal data	assignment of network access credentials differentiated by service / management and password customized; use of password protected screensavers in case of inactivity; all computers are covered by systems of detection and prevention of intrusions and anti-hackers, system firewalls,	ADEQUATE



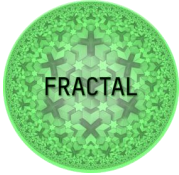
Project	FRACTAL	
Title	FRACTAL Cybersecurity features and requirements for Fractal	
Del. Code	D4.5	

	antivirus, antispyware whose effectiveness is periodically checked and updated;	
Unauthorized treatment (including modification, disclosure)	<p>each person in charge of processing is equipped with authentication credentials and / or password;</p> <p>the data must not be shared, communicated or sent to people who do not need it for it carrying out their work duties;</p> <p>backup copies come kept in a place not accessible to another person by the person in charge of the processing;</p>	ADEQUATE
Treatment not in accordance with the purpose of the collection or illegal	the personal data must be deleted before a possible reuse	ADEQUATE

TABLE OF VULNERABILITY and INTRINSIC RISK

Table 28: Calculation of Intrinsic risk

TYPE OF RISK	$RN = Ri \times V$	VALUE
Physical agents	$8 \times 0.25 = 2$	LOW ($1 \leq RN \leq 3$)
Natural events	$4 \times 0.25 = 1$	LOW ($1 \leq RN \leq 3$)
Service interruption	$6 \times 0.25 = 1.5$	LOW ($1 \leq RN \leq 3$)
Technical Problems	$12 \times 0.25 = 3$	LOW ($1 \leq RN \leq 3$)
Information Commission	$8 \times 0.25 = 2$	LOW ($1 \leq RN \leq 3$)

	Project	FRACTAL	
	Title	FRACTAL Cybersecurity features and requirements for Fractal	
	Del. Code	D4.5	

Unauthorized actions	$8 \times 0.25 = 2$	LOW ($1 \leq RN \leq 3$)
----------------------	---------------------	----------------------------

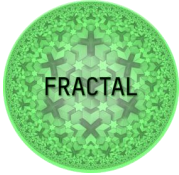
7.7.3 Phase 2 for that do not require DPIA (UC2, UC3, UC4, UC5, UC6, UC7 and UC8)

For their treatment there are no sensitive data to analyze, for this reason the risk assessment and the suitability of the technical and organizational security measures to make the risk acceptable is managed directly by the data controller.

7.8 DPIA results

7.8.1 Use case 1: Engineering & maintenance works

Downstream of the DPIA survey conducted, the activity falls into the **LOW** range.

	Project	FRACTAL	
	Title	FRACTAL Cybersecurity features and requirements for Fractal	
	Del. Code	D4.5	

8 Conclusions

In Section 4, a State-of-the-Art analysis of cybersecurity in embedded systems is done. This section helps understanding what the most common attacks are in embedded and IoT systems, focusing on the differences between commonly performed attacks on embedded systems with respect to typical attacks, i.e. physical attacks, tampering and physical access to the systems.

The importance of providing the IoT environment with a secure infrastructure and a robust networking is addressed in Section 5, introducing IoT API gateways as a mitigation for many of the most common network vulnerabilities, providing single entry-point features and security enforcement techniques like API authentication, IP restriction policies and load balancing capabilities. Then, a comparison between several IoT gateway alternatives is presented and Apache APISIX is proposed as the preferred choice, given its open-source nature, ARM devices portability and simple but complete configuration.

Section 6 implements a layer at the operating system level to protect the FRACTAL node against spoofing, tampering, denial of service and elevation of privileges risks. Failure to protect a system against these attacks can result in disclosure of confidential information, threaten the integrity of the node or deny its availability.

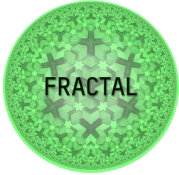
To prevent the occurrence of those cyber incidents in the Fractal node, a risk assessment has been carried out in accordance with ISO/IEC 27005. In the first phases of this methodology, an identification, estimation, and evaluation of risks is performed, indicating which assets to focus on according to their impact and their potential for attack and damage. The last phase of the methodology covers a risk treatment, where a set of countermeasures is implemented to address the most important security risks though the Fractal node.

All this work results in an OS Security layer corresponding the WP4T44-02 component of the Fractal project. This cybersecurity layer has been also verified for compliance with IEC 62443 standard.

Section 7 reports an analysis of GDPR compliance for all Use Cases involved in the project.

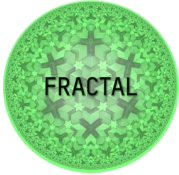
It started from a questionnaire, provided to each UC leader, whose purpose was to analyze criteria helping to identify impact on data protection. An analysis of the context and the data treatment was made in order to identify risks in each Use Case field together with the partners involved. Risks where evaluated and suggestion for mitigation were provided.

The main contribution in that activity was the possibility to share knowledge and issues related to data protection with all partners involved and to sensitize technicians about the impact on personal data.

	Project	FRACTAL	
	Title	FRACTAL Cybersecurity features and requirements for Fractal	
	Del. Code	D4.5	

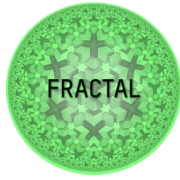
9 List of figures

Figure 1: Attacks on embedded systems.....	11
Figure 2: Information security risk management based on ISO/IEC 27005:2018 ..	15
Figure 3: Elements in the STRIDE methodology	17
Figure 4: Type of vulnerabilities according to the STRIDE methodology	18
Figure 5: Asset diagram	32
Figure 6: Verification results of the Yocto OS	45
Figure 7: Activity workflow	48
Figure 8: Treatment flow for UC2	55
Figure 9: Treatment flow for UC3	57

	Project	FRACTAL	
	Title	FRACTAL Cybersecurity features and requirements for Fractal	
	Del. Code	D4.5	

10 List of tables

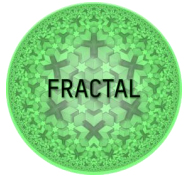
Table 1: T4.4 developed component summary	7
Table 2: Desired properties related to the STRIDE threats	17
Table 3: API Gateways comparison	21
Table 4: Use cases analysis	29
Table 5: Asset description.....	32
Table 6: Damage Potential.....	34
Table 7: Attack Potential	36
Table 8: Risk Evaluation	39
Table 9: Countermeasure description	41
Table 10: Countermeasures and related assets	41
Table 11: List of Personal Data.....	46
Table 12: List of Requirements.....	50
Table 13: Part of Questionnaire for UC1	68
Table 14: Probability values.....	72
Table 15: Consequences values.....	72
Table 16: Matrix combination of probability and consequences.....	73
Table 17: Intrinsic Risk values.....	73
Table 18: Vulnerability values	73
Table 19: Matrix combination of vulnerability and intrinsic risk.....	74
Table 20: Normalized risk values	74
Table 21: List of danger, risks, probability and consequences.....	74
Table 22: Risk 1 with consequences and level of risk.....	76
Table 23: Risk 2 with consequences and level of risk.....	76
Table 24: Risk 3 with consequences and level of risk.....	76
Table 25: Risk 4 with consequences and level of risk.....	76
Table 26: Calculation of Intrinsic risk	77
Table 27: Risks, measures and suitability	77
Table 28: Calculation of Intrinsic risk	78



Project	FRACTAL	
Title	FRACTAL Cybersecurity features and requirements for Fractal	
Del. Code	D4.5	

11 List of Abbreviations

Term	Meaning
AI	Artificial Intelligence
API	Application Programming Interface
ARM	Advanced RISC Machine
CIA	Confidentiality, Integrity, and Availability
CM	Countermeasure
CV	Computer Vision
DPIA	Data Protection Impact Assessment
EDP	Energy-Delay Product
FPGA	Field-Programmable Gate Array
GDPR	General Data Protection Regulation
HW	Hardware
IACS	Industrial Automation and Control Systems
IEC	International Electrotechnical Commission
IoT	Internet of Things
ISA	Instruction Set Architecture
IT	Information Technology
MMU	Memory Management Unit
NOC	Network on Chip
OS	Operating System
PULP	Parallel Ultra Low Power
QoS	Quality of Service
RBAC	Role Based Access Control
SoC	System on Chip



Project	FRACTAL	
Title	FRACTAL Cybersecurity features and requirements for Fractal	
Del. Code	D4.5	

SSH	Secure Shell
STRIDE	Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privileges
SW	Software
UAV	Unmanned Aerial Vehicle
UC	Use case
WCET	Worst Case Execution Time
WSN	Wireless Sensor Network